Amazing Algebra

Group theory and its applications

Everything is mathematical
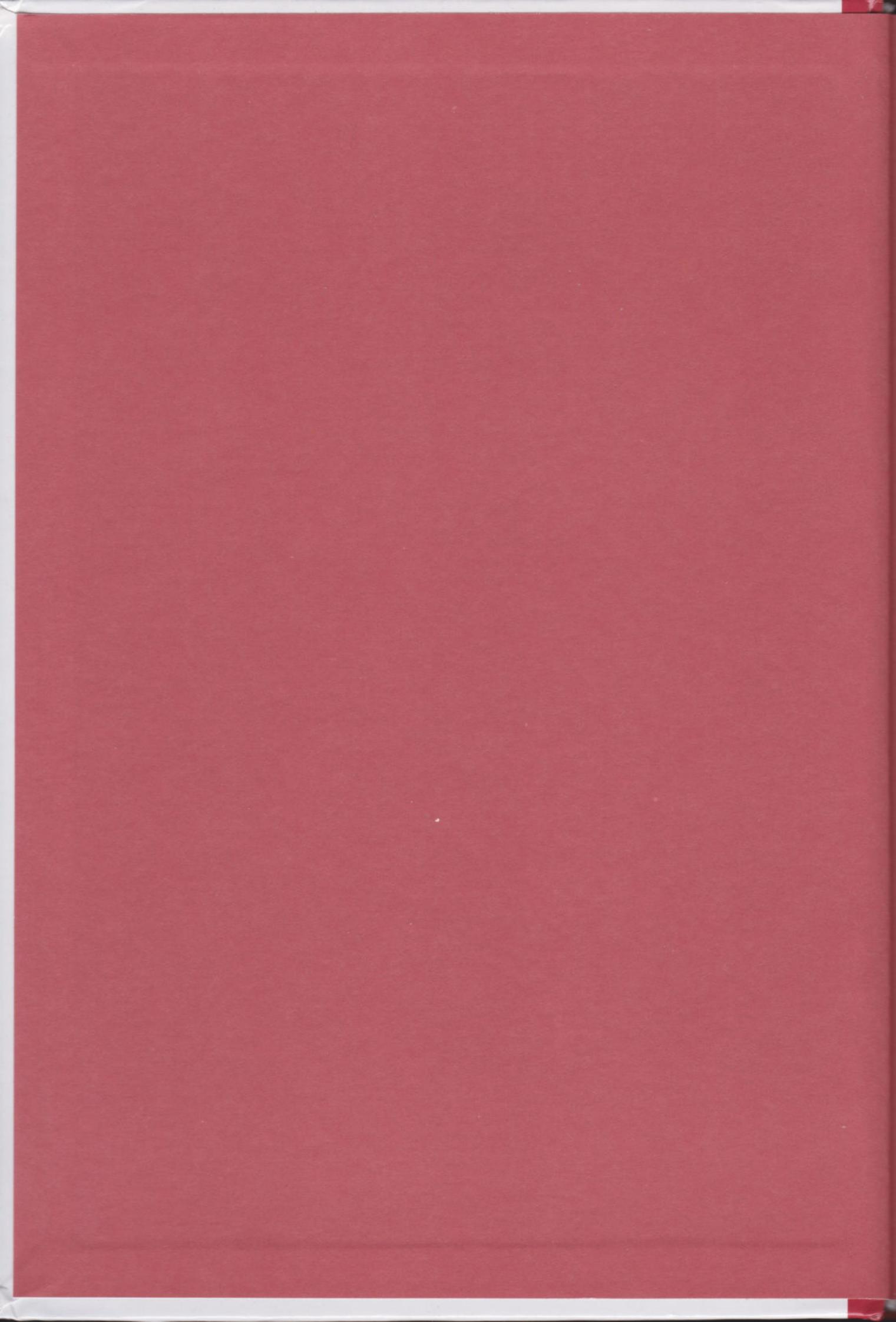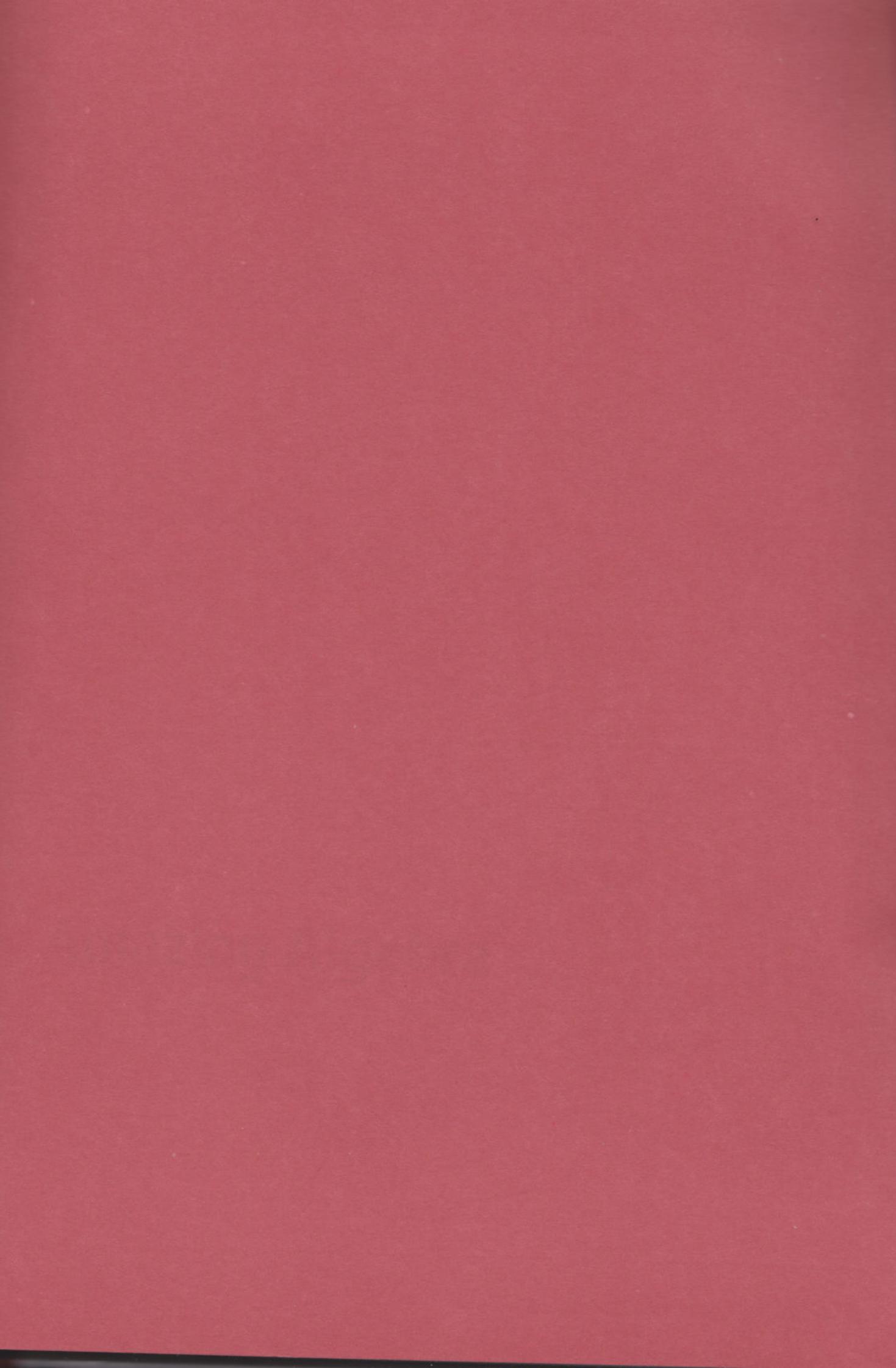
Amazing Algebra

Amazing Algebra

Group theory and its applications

Javier Fresán

Everything is mathematical

For Laura Casielles

Contents

Contents

Preface

New York, 1941. As it was 'midnight in the century', two extraordinary Jews could only continue their research under the protective cloak of the Statue of Liberty. André Weil, founder of the Bourbaki group, would revolutionise mathematics with the discovery of the equivalent of the Rosetta stone that made it possible to decipher some of number theory's most profound mysteries. While Weil travelled these seas of thought, Claude Lévi-Strauss would put an end to the image of the anthropologist as an explorer searching for adventure, thanks to the structuralist method. They met during a period of exile that left them alone with their intelligence. At the time, Lévi-Strauss was writing his thesis on the structures of kinship: everything was going as planned, until he came to analyse the marriages of the Murngin tribe, governed by rules so complex as to invalidate all known study techniques.

This book recounts how Weil made use of group theory, a branch of mathematics born during the previous century for understanding algebraic equations, to solve the problem that kept Lévi-Strauss awake at night. A group is a set with an operation that associates a third element to each pair of elements in such a way that certain conditions are satisfied. Numbers express quantities; groups measure symmetry. Hence, it is not strange that they are ubiquitous, not only in mathematics, but also in nature. If Henri Poincaré stated in 1881 that "mathematics is just a history of groups," today we can take a step further to claim that even quartz crystals or hydrogen atoms are governed by groups. As we shall see, the same holds for musical harmony and data protection systems that allow us to carry out secure bank transactions.

From the outset, it was clear to me that the history of the collaboration between Weil and Lévi-Strauss could only be explained by means of a dialogue. However, this raised an obvious problem: by setting the plot in New York in the 1940s, it would be necessary to dispense with everything that came after. It was then that I remembered a beautiful Jewish tradition that Weil's daughter mentions in a recent family portrait: the study companion with whom the dead continue to learn from beyond the grave. Claude Lévi-Strauss, who died in 2009, would be the classmate André Weil had been waiting for since his death 11 years earlier. *Sic rebus stantibus*, a word of warning is in order: I would not like anyone to be deceived by seeing a mask of fiction in the dialogic structure. Save for a few exceptions, every word of the protagonists is documented in the literature.

The origin of *Amazing Algebra* is the lecture I gave in August 2010 at the Universidad Internacional Menéndez Pelayo as part of the "fascinating Renaissance

Academy" that is the Aula de Verano Ortega y Gasset. I could not hand the floor to the protagonists without expressing my gratitude to those who organised the course, and those who have given me their time: Giuseppe Ancona, Gustavo Ochoa, Guillermo Rey, Roberto Rubio and Lucas Sánchez Sampedro. Thanks to them, the book moved a little closer to its goal: offering the general public an account of group theory through the work of André Weil and Claude Lévi-Strauss.

Chapter 1

The Bourbaki Years

Every mathematician worthy of the name has experienced,
if only rarely, the state of lucid exaltation in which one thought
succeeds another as if miraculously, and in which the unconscious
(however one interprets this word) seems to play a role.

A. Weil, *The Apprenticeship of a Mathematician*

The end of October, 2009

WEIL: You're 11 years late…

LÉVI-STRAUSS: A pleasure to see you, Mr Weil! I would have preferred it to be under different circumstances, but I'm pleased to have you as my study companion. I have many things to ask you!

WEIL: Me too, so without further ado let's get started on the main point: how did you manage to live to 100?

LÉVI-STRAUSS: The Indians taught me, and it would be imprudent to reveal their secrets, don't you think? It is funny we should meet again here: I recall that we once realised our ancestors might have known each other and that both your father and my own were *dreyfusards*[1] in their youth. I come from a family of Alsatian Jews who moved to Paris with the annexation because they wished to continue being French. Yours did the same, no?

WEIL: Only the paternal branch, the Weills, who lost the second letter 'l' somewhere along the way. Proust's mother, who was called Jeanne Weil, may have been related to us, who knows. The other half of the family came from the Galician steppe. These were the Reinherz, a name that means 'pure heart' in German. I heard many stories about them in my childhood. However, I didn't discover I was Jewish until the age of ten, and when I did, I gave the matter no importance.

---

1 Supporters of Alfred Dreyfus, the French soldier of Jewish origin who was unfairly condemned at the end of 1894 for the crime of high treason.

LÉVI-STRAUSS: Your sister, the philosopher Simone Weil, did not take the same position…

WEIL: You already know very well, Mr Lévi-Strauss, that she was exaggerated by nature, always trying to become a parachutist or hiding Trotsky in the house. At the age of 15, she had a crisis because she regarded her intelligence as mediocre. It is common among children of that age, but she thought of taking her life. In spite of all this, she was always a happy woman. We were inseparable as children. I'll never forget one afternoon when I fell over and she ran back home to find my algebra book to console me. She kept these moments of innocent tenderness for the rest of her life, but always understood things better than the majority of her fellow travellers. She was, for example, one of the first to attempt to open the eyes of the world to the situation in the USSR. Just when I thought nothing she could do would be able to surprise me, her death left me in tatters. It took me months to get out of my head that page from the memoirs of the duc de Saint-Simon which is cut in two by a stream of tears.

LÉVI-STRAUSS: During World War I, your father served in the military hospitals of the front and the whole family travelled with him on his postings. Did this not affect your education?

WEIL: I would say that not following the conventional system had only positive effects. I have always believed it is enough to have a good teacher every two or three years to give you the impulse to continue studying on your own. Einstein asked teachers not to teach anything that one had not already learnt on one's own. There are two teachers that stand out in my mind, particularly in my early years. I am sure that Mr Colin did not know any more about mathematics than he needed to explain, but I have not met anybody who could promote the imagination and rigour of students like him. He would ask somebody to come to the blackboard to solve a problem, and the whole class would spend ten minutes reflecting in silence. Then we would look for the solution together. It mattered little that our ideas didn't lead anywhere, but it was forbidden not to know the definitions by heart. Another of my schoolteachers had invented a sort of algebraic notation for grammatical analysis, which produced a fond feeling of reminiscence when I came to read Chomsky many years later.

LÉVI-STRAUSS: With this background, there is nothing strange about the fact that your years of education were, above all, years of pilgrimage….

WEIL: I travelled as much as I could. At the age of 19, they gave me the opportunity to spend a whole year in Rome, where a brilliant school of algebraic

geometry had been formed. Francesco Severi explained the theory of surfaces, and Enriques invited me to his house on a number of occasions, together with other students. It was on one of these occasions that I discovered the memoir of Louis Mordell on the rational points of elliptic curves, without which it would have been impossible to complete my thesis. The following year, one of the mathematicians with whom I'd made friends there, Vito Volterra, recommended me for a scholarship from the Rockefeller Foundation, which proposed to "raise the peaks" again after the ravages of war. I chose to visit Richard Courant in Göttingen the same year in which quantum mechanics was discovered (although I didn't realise that until later on!) and I also spent a few months in Berlin. I still had time to help Mittag-Leffler, who was struggling with an article on polynomial series. It was the thaw season in Stockholm. Every day we began by discussing mathematics in French, then my host changed the subject and began to talk in German; then he grew tired and gave a long monologue in Swedish, which invariably resulted in the phrase "Ah, I forgot you don't understand Swedish. We will continue tomorrow." As you can imagine, we made little progress with the manuscript during those weeks, but at the end of my stay, I was able to manage a conversation in Swedish without any problems.

LÉVI-STRAUSS: All this came before India?

WEIL: Yes, but I was already enthusiastic about the country. I think it was the preface to an English dictionary that discussed the Indo-European language that first led me to become interested in Sanskrit. And that was the source of a long-held dream of reading a literature that combines the most purifying refinements of logic, grammar and metaphysics with a mysticism brimming with sensuality in its original language. I began to attend the Sanskrit classes given by Sylvain Lévi at the Collège de France[2], and it was actually him who allowed me to spend two years in India. My trip came in the context of a plan for renewing the teaching body of the Muslim University of Aligarh, which, except for a handful of honourable exceptions in history and philosophy, was totally mediocre. Even if the academic world is never without intrigue, those I discovered there would exceed even the wildest imagination of an author of *feuilletons*. You should remember, Mr Lévi-Strauss, that as the youngest in the department – at the time I was 20 years old – I was assigned the task of writing a report on each teacher, which could, in the worst case, result in

---

2 Founded in 1530 by King Francis I, the Collège de France is unique in the world. Each of the holders of its chairs in the sciences and the humanities organise high-level courses open to the public that present 'research in the making'.

André Weil, together with his daughter Sylvie, in 1956
(photograph by Konrad Jacobs, courtesy of MFO Picture Collection).

their dismissal. All of them were worthy of being dismissed, but in the end I ended up suggesting that they replaced just one of the assistants with a student of Hardy, the only mathematician, in the strict sense of the word, among the more than 100 candidates for the position. I also assumed responsibility for purchasing a library collection for the university and attempted to establish a school of mathematics.
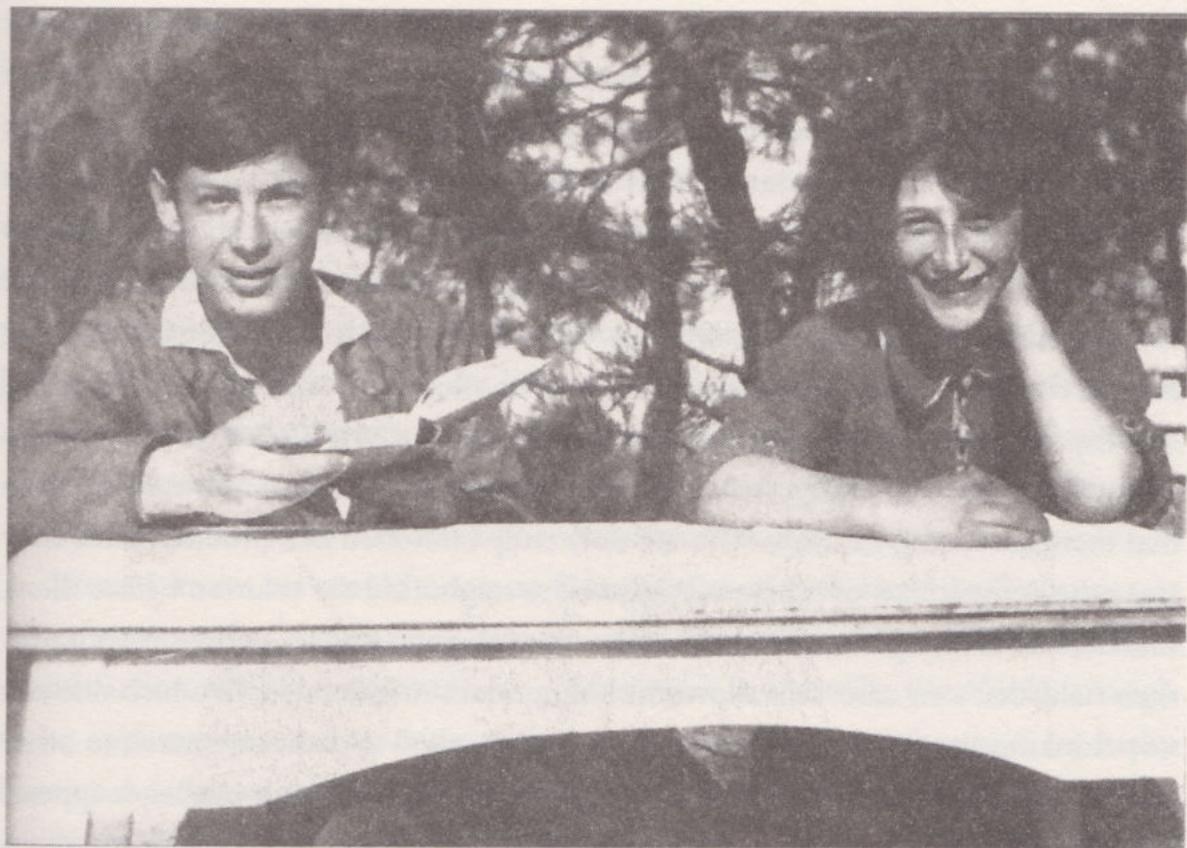
*André Weil, with his sister Simone,
reading in the countryside in the summer of 1922.*

However, it is difficult to change what is established, even with the support of the younger generation.

In order to tackle each obstacle with renewed vigour, I explored the country in my holidays. The railway guide soon became my bedtime reading. I always travelled by train, with little more than the *Iliad* and *Bhagavad-Gītā*, two books that have accompanied me since then and have allowed me to better understand the thought of my sister. On one of these expeditions, I met Gandhi, who began his salt march shortly after my arrival in India; on another, I met the poet Rabindranath Tagore, and a future president of the republic. By crossing paths with people from all walks of life, I observed some extremely curious analogies. I had often heard people talk of the parallels between the Talmud and psychoanalysis. I realised that the Brahmans from the south of India played the same role as the Jews in the European intellectual landscape. They had also dedicated their lives to giving commentaries of sacred texts in minute detail and, in their case, one of the reasons that they aroused such hatred was the imbalance between their number and their importance.

LÉVI-STRAUSS: I cannot help but ask you, Mr Weil, among so much travel and reading, where did you find the time for research?

WEIL: You are not the first to point out, albeit in a friendly manner, that my memoirs are like the chronicle of a *dolce far niente*… Perhaps that's why the editor thought it necessary to warn readers that they would find more "life" than "mathematics". It is possible, but that 'golden age' ended at 26. Ask the doorman of my apartment in Chicago what my pace of work was like in the following decades. After seeing me at the typewriter afternoon after afternoon, until late into the night, one day he could not help but remark: "You work a lot, Mr Weil. If you keep it up you will become famous." If what you are looking for is a justification, I'll tell you that there are mathematicians who are only truly interested in a problem once they sense the competition of other colleagues who might find the solution before them. Others, however, feel more comfortable when there are fewer people working in their field: that's my case. This allows for long periods of reflection, in which one can stop thinking about the problem – at least consciously – to dedicate oneself to other matters and return to it later with a fresh mind. To continue with oracles, it appears to be the case that, shortly after meeting me, Courant remarked to one of his students that I would be a brilliant mathematician, but a terribly *unproduktiv* one. Today, I would have told him Italo Calvino's story from China in which the king asks a painter to draw a crab. The artist replies that he will need five years and a house with 12 servants. When the five years were up, he still hadn't finished the painting. The king gave him another five years, which ran the risk of ending in the same way. However, at the last moment, the painter took the brush, and in an instant, with just a single movement, drew a crab – the most perfect crab that had ever been seen.

LÉVI-STRAUSS: While we're talking about animals, are there also foxes and hedgehogs in mathematics? These are the two classes of thinkers and artists distinguished by Isaiah Berlin, freely interpreting the line from the Greek poet Archilochus: "The fox knows many things, but the hedgehog knows one big thing". Hedgehogs have a systematic and centralised vision of the world that gives meaning to individual events. Foxes, on the other hand, believe that an isolated event can be consistent, but that everything is dispersed and multiple, and cannot be captured from instant to instant. Berlin includes Plato, Dante, Nietzsche and Proust among the former, and Aristotle, Shakespeare, Montaigne and Joyce among the latter.

WEIL: We have eagles and sparrows; these were the words used by Severi when I asked his opinion on one of the most brilliant mathematicians of the time. Eagles create concepts that open paths to be sailed among the islands of the mathematical

archipelago; their standard is metaphor and analogy. Sparrows, on the other hand, find beauty in examples; it can be said that they are the echo chamber of a sound that is not their own, but that theories advance thanks to them. Although it is not for me to classify myself, I feel like I am an eagle, perhaps on account of my inheritance. My teacher Jacques Hadamard instilled in me the desire to know more than non-specialists and less than specialists, who are often unable to solve a problem because it requires techniques from other areas that they completely ignore. Just as in a mountainous landscape, the rays of the Sun are hidden behind distant ridges, of which we are scarcely able to form an idea, when it comes to writing, it is necessary to make an effort to allow the reader to discover new perspectives behind the obvious argument.

LÉVI-STRAUSS: Bourbaki was a phenomenon of eagles…

WEIL: I knew we would come to Bourbaki sooner or later! To be precise, it was a sparrow that transformed into an eagle. Everything began with a sense of dissatisfaction when it came to teaching. After a year in Marseille, I was lucky enough to be appointed to the teaching staff at the University of Strasbourg. I say lucky because, in contrast to other provincial cities, the capital of Alsace had an extremely active intellectual scene and an excellent library, which almost certainly inspired the art historian Aby Warburg in the design of his own. My friend Henri Cartan, with whom I had studied at the École Normale Supérieure[3], was already teaching there; we both gave a course on differential and integral calculus. The custom was to follow Goursat's textbook *Cours d'analyse*, but to us it seemed out of date. I recall that Cartan subjected me to a series of questions that were so exhausting that I began to nickname him the 'Grand Inquisitor'. I was also interested in other issues, such as the level of generality with which the Stokes' formula should be taught. One day at the end of 1934, I had an idea: I went to see Cartan and I said to him, "Look, there are quite a few of us on this course who taught at various French universities. Let's get together and decide once and for all how to design the curriculum!"

LÉVI-STRAUSS: That was the birth of Bourbaki…

WEIL: Yes, but none of us could have imagined it. The others were Jean Delsarte, who taught at Nancy; Claude Chevalley, the only Frenchman interested in number theory in addition to myself; Jean Dieudonné, who later became the secretary of the group; and a few more who subsequently left. Some people call us the "founding

---

3 The *École Normale Supérieure* in Paris is a prestigious higher education institute that educates professors and researchers in all disciplines of the sciences and humanities. It has produced 12 Nobel laureates and 11 Fields Medal winners. To be admitted to the institute, students must study in so-called 'preparatory classes' for two years, before sitting an admissions exam that includes various written and oral tests.

fathers". The first meeting took place in a café in the Latin Quarter of Paris, on the corner of the Boulevard Saint-Michel and the street that goes up to the Panthéon. As I have already explained to you, our goal was to write a book that would serve as a reference work for the next 20 or 30 years. We soon decided that, in a collective work such as this one, it would not be appropriate to display a list of names on the front cover. It was then that we remembered a joke some of us had witnessed at the École Normale Supérieure: passing himself off as a foreign teacher, with a false beard and an implausible accent, one of the students gave a ridiculous lecture to the first-year students, which ended with the 'theorem by Bourbaki'. He had taken the name from an obscure general of Napoleon who, in spite of his promising start in the Crimean War, suffered a humiliating defeat at the hands of the Prussians that drove him to attempt suicide. Bourbaki would be our name! All we had to do was invent a back story. We decided to call him Nicolás and give him Poldevian origins. Another joke by some of those from the École was to launch a campaign in support of the fictitious state of Poldevia, which was so poor that its prime minister did not even have enough money for clothes. With the connivance of Élie Cartan, the father of our classmate, we published a note signed by Nicolás Bourbaki in the proceedings of the Academy of Sciences. Much later, he was introduced as a descendant of the general, ensuring that a whole family tree had been reconstructed and that… there were no mathematicians in the family!

LÉVI-STRAUSS: How did this discreet beginning transform into an encyclopaedic thirst to unify all of mathematics?

WEIL: As we worked on the project, we realised that, in order to provide a rigorous foundation for differential and integral calculus, it would be necessary to go back and examine the most basic concepts of mathematics from first principles. For earlier writers, it had sufficed to present just what was needed to begin the study of their works in a few chapters. However, this was not possible if we wanted to keep abreast of the extraordinary progress of our time. You must remember, Mr Lévi-Strauss, that mathematics is a relatively good fit to Thomas Kuhn's theory of scientific revolutions. Between the end of the 19th century and the first third of the 20th, a paradigm shift had occurred: the period saw the birth of Cantor's set theory, Hausdorff's general topology, Poincaré and Lefshetz's algebraic topology, Hilbert spaces, and modern algebra, which can be associated with names such as Noether, Artin and van der Waerden. All starting periods are the same: they begin with the analysis of many examples, which are considered in isolation until somebody comes to classify them, such as the first naturalists, in line with the most clearly visible

analogies. Hidden properties can only be discovered by a calm analysis, and some may remain hidden for a long time. The goal of Bourbaki came to be making these recent constituent parts of mathematics visible.

Lévi-Strauss: Beginning with what Kuhn would call "normalised science".

Weil: The hardest thing was to find a method for working. In the beginning, we met regularly in the cafés of Paris, but these meetings soon became too short, and we decided to take two weeks of summer holidays together in agreeable surroundings – mathematics in the wild. The first conference took place in July 1935 in Besse, a small town in the Auvergne, where the University of Clermont had facilities. The next would have been held in El Escorial but, after we organised the meeting, the Spanish Civil War broke out. In the end, we had to meet in the Chevalley family home in Chançay, although it was still referred to as the 'El Escorial congress'. Before each meeting, we asked the members to write reports on various matters that formed part of the treatise. Once we had arrived, we read them together and sketched out a plan of what would be contained in each volume and how this would be related to what had already been published or what we would write in the future. The drafting phase then began. Since we had established the rule that the decision to declare a text as complete could only be taken unanimously, sometimes endless numbers of versions of each manuscript circulated for more than five years; we were never all happy. I still can't believe that in 1939 we had completed a fascicule of some 40 pages with the main results of naïve set theory, and that we found a publisher willing to publish it.

Lévi-Strauss: Calling the theory naïve was another one of your jokes?

Weil: Absolutely not. If we had wanted to summarise in one phrase the principle with which the Bourbaki book undertook its enterprise of unifying mathematics, it would be "putting the axiomatic method at the service of the ideology of structures". We shall come back to this later, Mr Lévi-Strauss. With respect to the method, we decided to base everything on set theory, which, in spite of the paradoxes it may have been plagued by at the start of the century, was in excellent health by the time we came to make use of it. Hence, the first step to formalise mathematics involved providing an exhaustive description of the symbols and syntax of set theory. Any one of the labours of Hercules would have been easier; we had the precedent of Russell and Whitehead, who invested 10 years of their lives, working around 12 hours a day, in writing the *Principia Mathematica*. However, by introducing a considerable number of abbreviations and new syntactic conventions, it was possible to obtain a much more practical language, which, without being formal in the strictest sense, would be sufficiently close to formal languages to guarantee perfect rigour. That is the source

of the naivety in the theory, a sort of stenographic version of the ideal language in which there were no loose ends. We soon abandoned formalised mathematics, but left signs along the way so as to be able to return when required. This forms the context of our obsession for naming conventions, the austere style, without rhetorical concessions; or a linear order that prohibits any reference to other texts, although this leads to real numbers being constructed only after page 3,000…

LÉVI-STRAUSS: Don't the historical notes with which Bourbaki habitually closed each book contradict the desire to make a *tabula rasa* of the past?

WEIL: That is a different matter, Mr Lévi-Strauss. Note that there is nothing left to chance in the title of our treatise *Éléments de Mathématique*. On the one hand, there is a conscious use of the singular form of a name that is more common in the plural: we referred to "*la mathématique*" and not "*les mathématiques*", because we believed there was only one. On the other hand, there is a clear allusion to Euclid's *Elements* in the title. We also wanted to create a work that would continue to be valid for 2,000 years, and this could only be achieved if it was self contained. Imagine somebody in the future who finds one of our research articles. It would contain so many references to other texts, the majority of which would probably have been lost, that no matter how interesting it was, it would be regarded as useless. To make a *tabula rasa* is not to deny that there were mathematics prior to us, just as there had been geometry prior to Euclid. Quite the contrary; our treatise, just like his, is a sum of what was known when we wrote it. However, what happens is that on many occasions, when old material is organised, new material is discovered.

I must confess that the idea of adding these historical notes to the end of each volume was my own; let me explain why. When I started at the École Normale, I found that the science library had ridiculous opening times. Fed up with my complaints, the director gave me a job as a library assistant, which provided me with access day and night in return for a minimal obligatory presence. It was there that I read the work of Bernhard Riemann, thanks to the German I had learnt in order to understand what my parents were saying when they didn't want me or my sister to hear. Reading his work convinced me of an idea that had already occurred to me from my discussions on the Greeks: in the history of humanity, the only people who matter are the geniuses, and the only way to discover them is by direct contact with their work. From then on, I have always advocated a history of mathematics grounded in reading the classics, and not in learning dates by rote that are of little importance to anybody.

LÉVI-STRAUSS: When you read the work of the great mathematicians of the past, were you not irritated that they were not as rigorous as your group?

WEIL: In fact, this was the great risk we ran; I suppose that we did not always know how to keep a distance. I had the privilege of learning history from Max Dehn, one of the two people in my life who have made me think about Socrates. This extraordinary teacher, who believed that mathematics was just one of the many mirrors on which reality is reflected – albeit perhaps more clearly than in others – organised a seminar at the University of Frankfurt. It had the none-too-pretentious goal of reading the great texts from the perspective of their author, without asking of mathematicians of the past what only the formalism of the present can offer. This is the programme that I followed later on in my book on the history of numbers – to show mathematicians in their workshop so that readers could see the thought process of the Babylonians of the times of Hammurabi, who engraved a list of Pythagorean triples in the Plimpton tablet, all the way to the Legendre of the *Essai sur la théorie des nombres*…

LÉVI-STRAUSS: That is the book that opens with Chinese calligraphy?

WEIL: The very one! I asked my colleague the mathematician Shiing-Shen Chern to write the Chinese proverb "the old horse knows the route" in his beautiful calligraphy, which is why the photograph of the bas-relief of the tomb of the emperor Taizong, which represents a horse, appears on the following page. I thought that this provided a good summary of my decision to focus on the history of mathematics, when active research was becoming increasingly difficult due to my age. You cannot imagine, Mr Lévi-Strauss, how many mathematicians have succumbed to depression in their final years because their minds were no longer as quick as in their prime; I didn't want this to happen to me, and so I became a historian. I'm talking about my personal experience of old age. The myth that associates youth and mathematics is only partly true: it is certain that there have been mathematicians who, in spite of dying extremely young, will always be remembered for their discoveries. However, it is impossible to put an arbitrary date on creativity. In *A Mathematician's Apology* Hardy mentioned 35. Is that not just because this was the age at which he no longer believed he would be able to prove new theorems? Without going into greater detail, I would say that my best work came after the age of 35.

LÉVI-STRAUSS: However, the 'retirement' age of the members of Bourbaki was perfectly established.

WEIL: And it was I who was responsible for ensuring it was respected! I don't know at what point we decided that nobody could exceed 50 years old. One of the

老馬識途

陳省身題
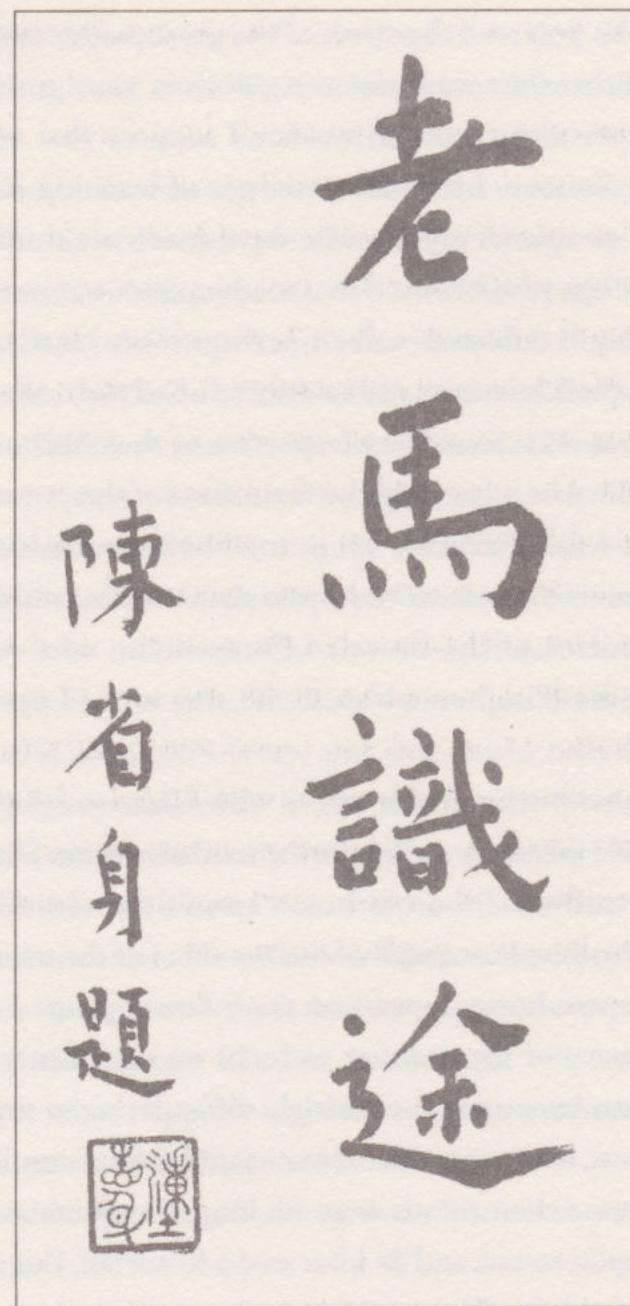
Chinese proverb: "The old horse knows the route."

keys to the success of Bourbaki was precisely this renewal across the generations: the best students of each year participated in our meetings as 'guinea pigs' and many came to be included in the group. There was an extremely important difference. While we had educated ourselves in ancient mathematics, they had been the first to learn from the new perspective; they were our students. I believe that French mathematics from the second half of the 20th century onwards would not have been so successful without this constellation of students who worked on the same topics of the books when they were being written.

LÉVI-STRAUSS: What was perhaps unexpected was that Bourbaki himself would die at the age of 50…

WEIL: In fact, it is not so surprising after all, Mr Lévi-Strauss. The vision we put forward is much better suited to firmly grounded disciplines, which have been tried and tested over time, than those that are still being developed. Although it is possible to give a formal definition of structure, the best way for me to understand it is to present it as an architectural metaphor. In fact, one of Boubaki's best-known titles was *The Architecture of Mathematics*. The structure is the way in which the different components of a building are brought together using joining elements that guarantee its stability. It is abstract. The function of a flying buttress, for example, does not depend on the material with which the vault is built. In mathematics, structures are used to permit the simultaneous study of all the objects with the same properties. It does not concern itself with their nature, but the relationships between them. Two objects that look completely different may be incarnations of the same archetype. When we have freed ourselves from all the superfluous accidents, what remains is the structure, something inert that we cannot transform. In Bourbaki we decided to base all the structures on set theory. However, it may be the case that the time has come to reconsider this. It may perhaps even be time to consider whether it is possible to continue speaking of a single mathematics.

Chapter 2

Elementary Structures

Anthropology is, with music and mathematics, one of the few true vocations; and the anthropologist may become aware of it within himself before ever he has been taught it.
C. Lévi-Strauss, Tristes tropiques

WEIL: I must confess, Mr Lévi-Strauss, what most surprises me is that someone as intelligent as you studied philosophy.

LÉVI-STRAUSS: Sins of my youth, I fear; although I abandoned it at an early age to dedicate myself to ethnology. You are the one who has turned into a philosopher with the passing of the years. Need I remind you about your article *From Metaphysics to Mathematics*?

WEIL: I would call that a 'history of ideas'. If you had read the text, you would know that mathematicians in the 18th century used the term 'metaphysics' to refer to a series of diffuse analogies that could not be precisely formulated, but which guided their research. I don't think this says much in favour of philosophy.

LÉVI-STRAUSS: Call it what you wish, Mr Weil. Regardless, what led me to philosophy was a sort of opening onto the variety of the world that had accompanied me since I was a child. If there is something that distinguishes Jewish families — we both know this — it is their veneration of culture and intense interest in the intellectual life, which even remains when they have abandoned all their beliefs. To the adage 'merchant or rabbi', we should add that a businessman does not want his children to follow him to the top of the company. It is not the done thing to have two generations pass without academic success in his nuclear family. When the time came to choose a career, I had too many interests. I divided my time between painting, music and antiques. However, my father was a painter, and I had experienced his financial difficulties from up close. Nor did I have sufficient talent when it came to music, although I would have liked to have been the conductor of an orchestra. I thought that by studying philosophy, I would not

be forced to separate myself from my passions to the same extent that would have been required by other disciplines.

WEIL: You are forgetting about politics…

LÉVI-STRAUSS: Of course! At that time, I was extremely militant; what really interested me was politics. It makes me laugh to remember that for many years I dreamt of becoming the new philosopher of socialism! It all began on my holidays one year when I met Arthur Wauters, who would go on to be the Belgian ambassador in the USSR. It was he who made me read Marx and who put me in contact with the leaders of the Belgian Workers' Party, who showed me all the cooperatives and Houses of the People. On my return to Paris, I gradually carved out a space in the French Section of the Workers' International – first in small committees, then as a representative of the young student socialists. I even became a candidate in an election, but my campaign ended with an accident a few hours after it had began. We were driving a Citroën 5 CV, although I didn't have a driving licence, and it was the first time I had been behind the wheel of a car. I was not setting a good example…

WEIL: You should be grateful for the accident, they might have elected you. What I don't understand is how somebody who was so committed during their youth would not sign the "Manifesto of the 121" against the war in Algeria later on.

LÉVI-STRAUSS: At the age of 20, I would have gone round the doors in person collecting signatures. However, remember that when the war broke out, I was immersed in writing *Tristes tropiques*. I first signed a letter, published in *L'Express* in November 1955, in which we requested the creation of a committee for finding peace in Algeria. Some years later, they asked for my support in what would go on to become the "Manifesto of the 121", although they already had names such as Sartre and Simone de Beauvoir, alongside many others. However, the fame that was being sought for the manifesto was, in my case, the result of a series of ethnological studies, and there are no two rhythms that are more different than science and politics. Upon analysing the details of an indigenous population, I felt bound not to write a single word I did not consider correct, or at least well founded. This prioritisation of the truth was at odds with the political judgements that were in vogue in those years, which made me think the best way to resolve a contradiction that had begun to torment me somewhat would be to retire from public opinion altogether. And you, what did you do against the war?

WEIL: I can't believe you're asking me, Mr Lévi-Strauss! Do you not know the story? In 1939 I was a reserve official and had made up my mind to desert if I was called up. I spent that summer with my wife Eveline in Finland: we were on the

banks of a lake beside the Russian border, and during the day we both worked on a boat – I on my report for Bourbaki; Eveline, on practising her shorthand. There was nothing strange about the fact that the locals thought I was a spy, and a file was opened on me at the police station in Helsinki. I didn't find out about this until the Russians dropped the first bombs on the capital. I was arrested and in the search they discovered suspicious invitations to the wedding of Bourbaki's daughter. I shudder to think that they might have executed me there and then. According to the account of the mathematician Rolf Nevanlinna 20 years later, this is how things happened. At a dinner he attended as a colonel in the reserve, the police chief went over to inform him: "Tomorrow we will execute a spy who says he knows you." Knowing they were talking about me, Nevanlinna requested that they limited themselves to expelling me from the country.

I was turned over to the Swedish authorities on the border, who swiftly repatriated me to France to complete my sentence for desertion in prison in Ruan. There is nothing more favourable to abstract science than a spell in prison. In the first letter I wrote to my family, knowing it would be read by anyone and everyone along the way, I made it clear that I would commit suicide if I was not provided with the resources required to work. From that point onwards, I had an individual cell and was never without a pen and paper. I think that Cartan was jealous. He once wrote to me "We do not all have the fortune of being able to work, as you can, without anyone bothering us." In the summer of 1940 my sentence was suspended in exchange for immediately joining the Cherbourg company, whose sole mission was to travel to the station every day to load buses. Now you can see that, in fact, I am a deserter. Let us be clear; I have never believed in the categorical imperative. There can be no universal behaviour, since each is governed by their *dharma*: just as Gaugin's lay in painting, I discovered mine in mathematics.

LÉVI-STRAUSS: And I thought that mathematicians were always the first to sign up to a revolution…

WEIL: What is certain is that, regardless of the regime, the work of mathematicians is too impenetrable for laypersons to allow it to be criticised from outside: if they remain united, they are invulnerable. Among my colleagues from Bourbaki, a number had extremely distinguished political lives. For example, Henri Cartan, who was very committed to the ambitious task of achieving reconciliation between the French and the Germans after World War II – it was something of an obsession. In 1946 he organised conciliation meetings in Oberwolfach, a small town in the Black Forest. Without him, the European Mathematical Society would not exist,

of that we can be sure. With respect to my friend, Laurent Schwartz, another of the members of Bourbaki, what more can I say except that I have never met a more skilful negotiator? He managed to maintain his critical independence with power and, at the same time, be treated with the greatest honour by the presidents of all sorts of governments. His memoirs are entitled *A Mathematician Grappling with His Century*. This is an extremely modest image: he was the century. He was a key figure in the opposition to the Vietnam War, as he had been before in the Audin affair[1]. My sister, who welcomed anybody who looked like a dissident communist Jew with open arms, would have been extremely proud of him.

LÉVI-STRAUSS: How time has passed! During the Vietnam War, I was not involved in politics at all. Better that way: I don't think my thesis that there are no societies without rules would have been very popular among those who took to the streets to shout "banning is banned".

WEIL: You are right, we digress. But it's not a problem when we have eternity ahead of us... Perhaps you would like to explain why you exchanged Plato for savages.

LÉVI-STRAUSS: The natural progression for students of philosophy was to sit the entrance exam to become a higher education teacher. After five years at the Sorbonne, this was not what I dreamed of. I was fed up with mechanically applying methods that only consisted of putting together words with similar sounds, such as essence and existence. The subject didn't matter, there were no references, everything was just combinatorics. We were a group of rebels who knew this all too well and who trained ourselves by applying the method to debates such as the superiority of trams over buses. However, the examinations represented a challenge. It was necessary to read a lot in an extremely short space of time; it was a sort of obstacle course through various doctrines. I still can't explain how I secured a position, in the same examination as your sister, by the way. She came seventh, and I came third, something that is even more inexplicable.

I spent my first year as a teacher in the Institute at Mont de Marsan, the capital of Landas. I must admit that I was extremely happy. Recently married, I gave classes on the fly, and everything was new, stimulating. However, the following year I was horrified at the thought of repeating the same course for the rest of my life.

---

1 Maurice Audin was carrying out his PhD in mathematics at the University of Algiers when he was kidnapped, tortured and murdered by the French authorities as a response to his anti-colonialist militancy. After he had gone missing, a reading of his thesis was organised in Paris *in absentia*.

Fortunately or unfortunately – I'm not sure which – my intelligence is neolithic: once I have cleared a space and cultivated it, what appeals to me next is to raze it and search for new spaces. I struggle to fix my gaze on the same object twice. It is the fear of repetition. To this should be added the certainty that my destiny was already fully determined. After marriage, children would come, and little by little, the whole family would move to a residential suburb on the outskirts of Paris. No! It was at that point that I received the call that would be my salvation. One Sunday in the autumn of 1934, at nine o'clock in the morning, I can remember it as if it were yesterday. It was the director of the École Normale Supérieure, Célestin Bouglé, phoning to offer me a position teaching sociology at the University of São Paulo. He needed the answer before 12 o'clock.

WEIL: But you were not a *normalien*.

LÉVI-STRAUSS: I was also surprised he called me. I had taken it upon myself to inform various friends of my desire to teach abroad, something which, at the time, was not as fashionable as it is now. Teachers were not very fond of travelling and I suppose there were few people in the conditions to take up the post. It matters little that I was not from their fold. In fact, Mr Weil, to begin with I had wanted to enter the École Normale, but I did not feel I was at the same level as classmates who were also preparing – they seemed like genuine monsters when it came to passing exams. As I didn't do well in Greek, I thought I could avoid it by choosing a subject in the sciences. This was mathematics, but the remedy only served to make things worse. After one year, I decided to leave and enrol at the university. My teacher thought I wasn't destined for philosophy, but for something akin to it. He wasn't completely wrong. In his opinion, it was law, although it turned out to be ethnography!

WEIL: At that time they were recruiting philosophers…

LÉVI-STRAUSS: That's right. Ethnology had practically no representation in French universities, hence the few people who worked in the field had received their education in another discipline. Many, like me, were self taught. Of course, it's certain that there was a precedent: Rabelais and Montaigne, for example, made use of an incipient ethnography to analyse the beliefs and institutions of their time. However, it would still be necessary to wait until the end of the 19th century before the Société des Observateurs de l'Homme was founded, which brought together naturalists always willing to undertake long journeys to collect myths and customs from other peoples, as if they were species of animals and plants. A method was missing – 'participant observation' – which was not introduced by the British school until the beginning of the 20th century. What

Claude Lévi-Strauss.
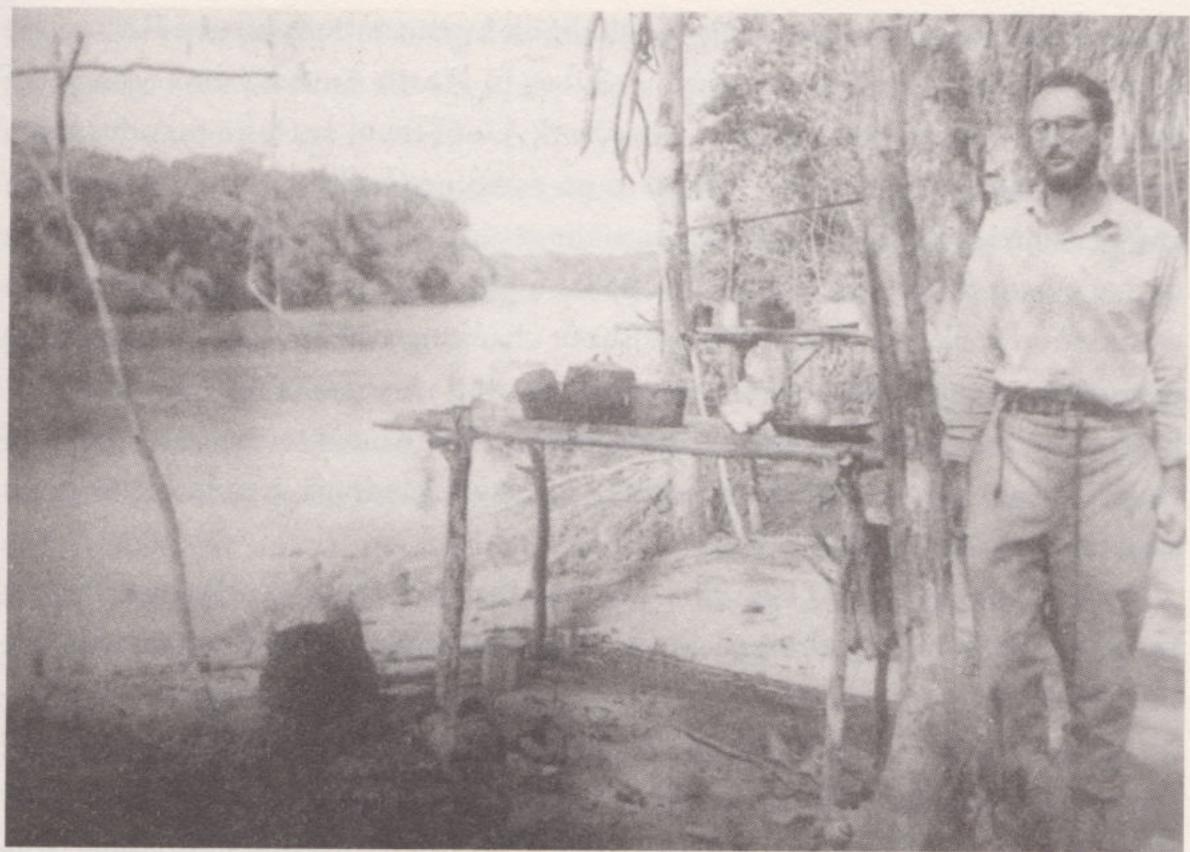
Two photographs of Lévi-Strauss during his expeditions in Brazil.

aroused my curiosity was reading an old book by the anthropologist Robert H. Lowie, who had lived among various tribes in North America and who years later would help me seek exile in New York. Until then, my taste for adventure had been somewhat discreet. I liked to go camping, walking in the mountains, and I even tried to convert the city into the setting for small adventures together with a group of friends. We would choose a point in Paris and a direction, and would then walk in a straight line, without changing course. This led us to have extremely peculiar experiences, but at best they were all trivial. When I read Lowie's book, *Primitive Society*, I immediately felt the need to discover the wide world. If they had proposed sending me to New Caledonia, I would have gone there too, without batting an eyelid.

WEIL: Nobody would say so having read the start of *Tristes trópiques*: "Travel and travellers are two things I loathe." Just as well you liked adventure, Mr Lévi-Strauss!

LÉVI-STRAUSS: There is something that should be kept in mind when we talk about *Tristes trópiques*, Mr Weil. I put off writing it for years. Notice that my last expedition to Brazil was in 1939, and I didn't start work on the book until 1954. When I returned from my trip, in the short time I had available to reintegrate myself into life in France before mobilisation for the war, I had begun to write a novel with the same title. However I gave up after 50 pages when I realised it was a poor imitation of Conrad. I don't have the imagination or patience required to invent the profile of a character with all its light and shade. I wanted to be a scientist, not a writer. Fifteen years later, I suffered a crisis in which I felt somewhat isolated both academically and socially. I didn't find my place. I remembered those early chapters and wanted to return to them as a sort of escape, although by that time the only thing that survived was the sunset at the end of *From a Log Book*. I wrote down what came into my head exactly as it came into my head. They were some fabulous distractions that lasted for four months.

WEIL: Maybe that's why Gallimard rejected the book...

LÉVI-STRAUSS: In fact what they rejected was a project I sent to them before writing it. They thought my idea was not quite mature enough. I think they regretted it immediately, when not long after *Tristes trópiques* was published by Plon, the Académie Goncourt issued a statement regretting it had not been a novel, since it would have won the prize! Anyway, what I was trying to explain is that it allowed me a freedom that would not even have occurred to me upon tackling my research. And this gives the book a different type of truth. One example of this freedom was

being able to say, without feeling the least bit guilty, that travellers and travelling are two things I loathe. After the war, there was a widespread tendency on the cultural scene – I suppose it has endured over the years – to attach value more to the exotic elements of ethnology than their conclusions, when for me, to spend weeks travelling, surrounded by danger and suffering from fatigue, to discover a new myth or slightly modify the known rules of marriage, was by far the least pleasurable aspect of my profession.

The tropics were not only sad as a result of the devastating effect of Western interference, but also because living alongside Indians was not enough to understand their culture. One could be awake from sunrise to sundown, trying to be unnoticed and showing an almost humiliating indiscretion while taking notes, but this was futile if the Indians had declared a silent war, as was the case in Campos Novos. It is a relief to think that the best fieldworker ever, Malinowski, a man of extraordinary sensibility, noted similar thoughts to mine in the diaries published after his death. I did not know this until a number of years later. On the ground, I consoled myself with the thought that I was collecting hitherto unknown human experiences that would soon vanish forever. In terms of humanity's heritage, their value was irreplaceable, but was all the effort worth it?

WEIL: Is this perseverance not a sign of art? Flaubert wrote *Sentimental education* 23 times. It was one of the first texts of his youth, and he rewrote it even just before he died. He was looking for the perfect page, in which all lives could be recognised. I'm sure that the differences between some of the versions are almost imperceptible. If we are talking about art, of course, this also includes mathematics. How many hours are spent proving a lemma that is only the first step on an uncertain road that may lead nowhere. And yet just one moment of lucid exhalation makes the whole process worthwhile. It is here that I need to cite Carl Friedrich Gauss, the prince of mathematics, who in a letter to the Italian Guglielmo Libri wrote "*procreare jucumdum sed parturire molestum,*" or in other words, "it is a pleasure to conceive, but giving birth is painful."

LÉVI-STRAUSS: For me, scientific pursuit with all the difficulties that go against it, with all the joys it offers, always evokes the image of an excursion to a plateau in Languedoc during my youth, in which I concentrated on following the boundary between two geological strata. They were not the incoherent movements that a mountaineer unaware of my intentions would have imagined upon observing me. If we know how to interpret it, the reading of a landscape can be just as rewarding as the finest literature.

Claude Lévi-Strauss
de l'Académie française

Tristes tropiques

Terre humaine
Poche

POCKET

Le grand livre de l'ethnologie
contemporaine
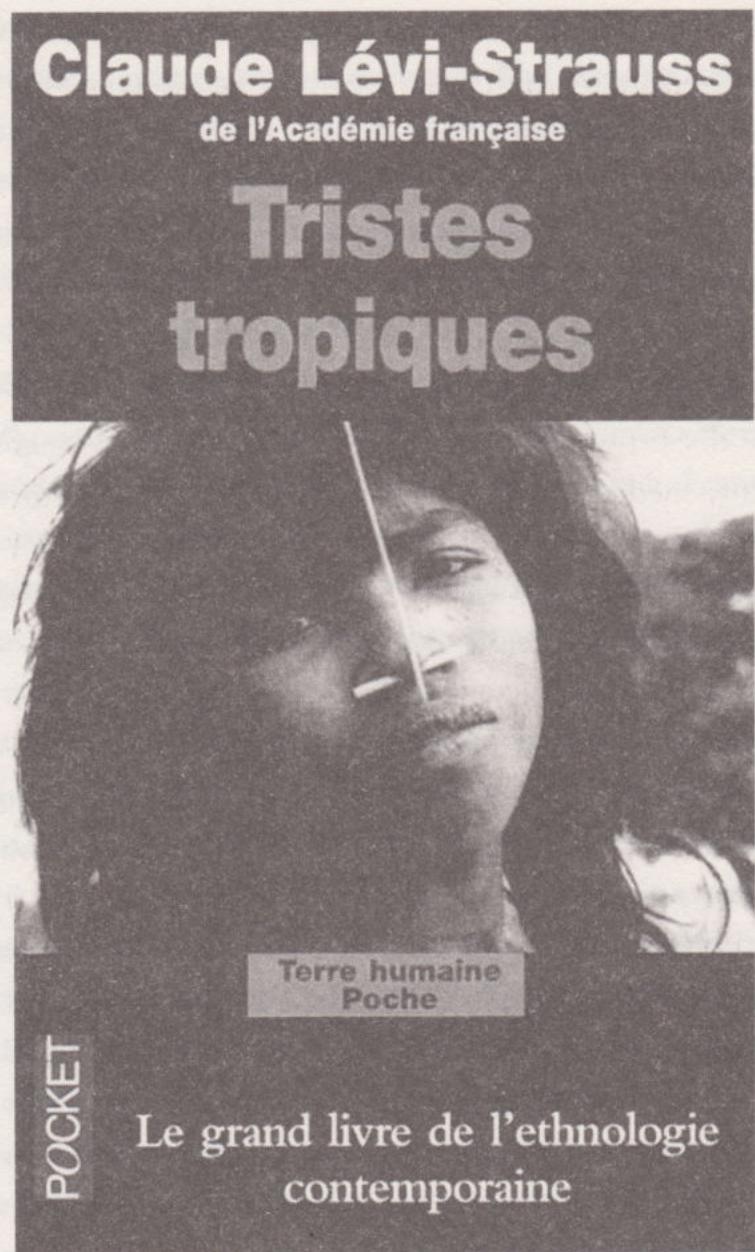
Cover of the French pocket edition of Tristes tropiques.

WEIL: I often think of the creative process as a long horse ride through wind and night, *"durch Nacht und Wind"*, that quickens as the objective is approached, just like the one Schubert set to music in his poem *The Elf King*. However, it should not be forgotten that sometimes only the child can see the Elf King, and the pace of the horse is reduced almost entirely although we are not yet out of the forest.

LÉVI-STRAUSS: Are you trying to say that from time to time problems escape even a genius such as yourself?

WEIL: Let me tell you something, Mr Lévi-Strauss. In my PhD thesis, I had developed one of Henri Poincaré's ideas that generalised a result of Louis Mordell. It

consisted of studying the rational solutions to equations of the form $y^2 = x^3 + ax + b$, referred to by mathematicians as *elliptic curves*. Starting from two solutions, Poincaré had found the way to obtain a third, but I shall explain this to you later on; I don't want us to get bogged down in the details. The important thing is that Mordell had shown that this procedure made it possible to recover all the solutions by starting with a finite number. I extended his result to more general curves, in which the polynomial that intervenes can be of any degree. It was not easy, since none of the methods of modern algebraic geometry existed at that time. I made haste to tell Hadamard and, satisfied with my work, I committed the indiscretion of telling him I believed my methods also allowed me to prove a conjecture that Mordell had stated in his article.

Hadarmard's reaction was the same as would have been expected of anyone who knew him. He drew close to me and said: "Mr Weil, many of us hold you in high regard. When it comes to writing your thesis, you cannot stop halfway, this is something you owe yourself. What you are telling me shows that your ideas have not matured sufficiently," just like those of Gallimard. Following his advice — for want of a better way of putting it — I focused all my attention on the Mordell conjecture. However, it was in vain, because nothing worked out as I had expected, and I ended up leaving it. *The Arithmetic of Algebraic Curves* — that was the title of my thesis — was published in 1928. Do you know how many more years would be needed to solve the problem? More than 50! Techniques that were not introduced until the start of the 1970s would play a crucial role in doing so....

LÉVI-STRAUSS: I'll confess that I haven't understood everything, Mr Weil; I hope you can explain it to me calmly another day. At any rate, the anecdote shows Hadamard at his best. I'm sure you remember his answer to me when I was working on *The Elementary Structures of Kinship* and I asked for his help: "Mathematics has just four operations. I don't believe marriage is one of these." Just as well I met you...

WEIL: Just as well, yes. Who knows who they would have given me as a study companion. Returning to *Tristes tropiques*, it's hard to deny your talent when it comes to choosing titles.

LÉVI-STRAUSS: I'm not sure my translators would agree. The titles only work in Romance languages. Every time my books were translated into English, it was necessary to sacrifice the word play: *Tristes tropiques* became *A World on the Wane*. What has waned is the music that seduced me so much when I planned to write the novel with this title. Also the flower of *La pensée sauvage* disappeared; a translation like *The Savage Mind* loses the polysemy that was essential to me

(*pensée* means both 'pansy' and 'thought') because what the book claims is that the science of the concrete, that untamed thought of savages, organises the world based on plant species.

Each title has a story, although the most amusing for me has been *The View from Afar*, a collection of articles I published in 1983. I had discovered the words of Jean-Baptiste Massillon, a French preacher from the 17th century, "The world viewed from up close does not hold up against itself, but upon moving afar, it becomes imposing." I told myself it was a fantastic epigraph for a book on ethnology, the title of which could only be *The View from Afar*. However, thanks to one of my colleagues, an expert in religious literature, I discovered that the quotation meant exactly the opposite of what I wanted to make the text say. In the language of the time, 'impose' meant to deceive, to confuse the senses. I had to renounce the phrase, but I kept the title, which continues to be one of my favourites.

WEIL: Without your experience in Brazil, none of these titles would exist.

LÉVI-STRAUSS: None! I remember that Célestin Bouglé had told me that the poor areas of São Paulo were full of Indians who could be observed in my free time; a sort of weekend ethnology. When I mentioned this to the ambassador in Paris, he burst into laughter. According to him, the last Indians in Brazil had been exterminated many years ago. He had no problem explaining how the Portuguese colonialists had tied them to their canoes before opening fire. It was a disappointment, since before I set out I still imagined the countries of the tropics as the perfect antithesis to the 'civilised' world. So strong was my conviction that I didn't even believe there could be a species that could be found in both corners of the planet.

What is certain is that both were wrong. There were no indigenous populations in São Paulo, but they could be found after a few days on the road. This did not stop me from undertaking small works of urban ethnography, which were particularly enriching in a city in which, in the space of just a few hundred metres, the Iberian colonial style could be found alongside landscapes more befitting Chicago, at the gates of modernity. By means of example, I surprised my students by asking them to reconstruct the history of the street in which they lived. My first contact with the Indians did not come until the summer holidays. During those four months in which the other teachers returned to France, my wife and I set out on our first expedition.

WEIL: In search of the Kaingang Indians, who were not as savage as you had hoped....

LÉVI-STRAUSS: It was just a taster. The Kaingangs had already had some contact with government authorities who had tried to show them the wonders of civilisation. It had given them beds on which to sleep, and they had burned them in an enormous fire. In some ways, my different expeditions represented an evolution towards the unknown, leaving my age behind to enter into another – the Kaingang, the Kadiweu, the Bororo, the Nambikwara, the Mundé and the Tupi-kawahib, each people was more primitive than the last. The Bororo expressed themselves in an extremely lively manner through the art of the feather, and their social organisation was extremely subtle, but they had also been touched by civilisation. On the other hand, spending a few weeks living with the Nambikwara Indians was an experience that blew me away completely. I noted everything down in a chaotic pile of notebooks impregnated with the strong smell of the creosote I used to protect myself from the insects.

A new idea came to me when I had only just had time to sketch out the previous one. I tried in vain to record the smallest details of the language, the music or the fishing techniques; they even allowed me to be present at a birth. I think that never until then had I responded better to the image given to me by a colleague during the boat journey that took us to Brazil: "A man with his eyes clearly open, but with all his being closed, as if he was scared of losing what he had just recorded". However, I was not so interested in the details as in understanding the idea of a human society reduced to its minimal expression. With the Nambikwara, the question posed by Rousseau in his *Discourse on the Origin and Basis of Inequality Among Men* or in *The Social Contract* could be understood from an experimental point of view: what is a minimal society?

WEIL: Allow me an analogy that may appear forced. We wanted to achieve the same with Bourbaki. The first three decades of the 20th century had seen extraordinary advances in set theory, topology and algebra, but the richness of the objects with which each of the disciplines dealt had not yet been exhausted. The theorems, for example, had not been stated as generally as possible, hence we set about the herculean work of finding the minimal structures that made them valid.

LÉVI-STRAUSS: What I was lacking then was the method. You must remember that my career was completely atypical. As a general rule, students received hundreds of hours of classes before their first contact on the ground; they knew the scientific literature but not the trade of fieldwork. I had already spent five years in swamps and with battle-hardened Indians at my back before I began to understand something

of the theoretical aspects. Suddenly, everything came together. Those were hectic months in which there was nothing else to do but read from the moment the New York Public Library opened until it closed.

WEIL: New York was a feast…

LÉVI-STRAUSS: The years I spent there are without doubt among the happiest of my life. We knew that the whole of Europe was collapsing, but the vitality of exile in New York allowed us to forget the pain. Sometimes 'pleasure masks memory'. I lived in a small apartment on 11th Street, which had nothing more than a bed, two tables and two chairs. That and my trunks from Brazil, to which I added totems from the Indians of British Colombia and other works of art I purchased in the antique stores on Third Avenue. When an anthropologist came to work with me, I gave him the bed and went back to my old explorer's customs, sleeping in a sleeping bag on the floor. Claude Shannon, the father of information theory, lived a few floors above, although I did not find out until a few years later. A Belgian neighbour told me there was a man trying to build an artificial brain, but I paid her no attention; who knows what they must have said about me. Did you realise how different these poor material conditions were from those I would later enjoy in my apartment in Paris? However, the Babel-like explosion of the city was like nothing I had ever known.

It was not easy to escape to New York. With the antisemitic laws of the Vichy government, I had lost my place in France. I first tried to go back to Brazil, but just as the ambassador was about to stamp my passport, one of his frowning councillors broke into the room to tell him that his power had been revoked; it was like something out of a spy movie. Luckily, the Rockefeller Foundation was able to invite me to teach at the New York School for Social Research, as part of its rescue programme for European scholars. I set sail on the Capitaine-Paul-Lemarle one morning in February 1941. There were 350 of us crammed onto the small steamship, with just two cabins. But I shouldn't complain after the horrors of the Holocaust. Furthermore, extremely interesting things took place on board. There was, for example, a Tunisian businessman carrying a Degas in his case. Victor Serge, the anarchist, who had written *S'il est minuit dans le siècle* (Midnight in the Century) two years before, was also present…

WEIL: I wonder why they used the conditional (*"s'il est"*). Primo Levi would also make use of it in his book *Se questo è un uomo (If This Is a Man)*. Perhaps the tense is the best expression of incredulity in the face of barbarity?

LÉVI-STRAUSS: Perhaps, I had never thought about it that way. At any rate, Victor

Serge and I were not particularly close. The great revelation of that journey was André Breton, who was travelling with his daughter and his wife. I'll never forget the moment I heard his name spoken when I disembarked from the ship in a port in Morocco. I was a great admirer of the Surrealists. Works such as *Paris Peasant* or the *Manifesto* itself were among my bedtime reading. I had even attempted automatic writing. We soon became friends and when, three months later (!), I was finally able to settle in New York, we kept in touch. Thanks to the Surrealists, I began to see a range of objects through different eyes, objects that until then seemed unworthy of art.

WEIL: While we're on the subject of automatic writing, let me tell you that for a while – although this would come later on – members of Bourbaki flirted with Oulipo, the Workshop of Potential Literature founded by François Le Lionnais and Raymond Queneau around 1960. It was a group of writers and mathematicians looking for new forms and structures for literature. They imagined words as points, phrases as line segments and paragraphs like planes. This led them to ask: what use is it to know that, given a phrase and a word that does not appear in it, it is always possible to form another phrase that contains it without sharing any of the words from the original phrase? They composed their poems dictionary in hand. Starting with a known text, they replaced each word by the following entry. For example "cabaret of love" becomes "cabbage off low". The approach revealed the hidden alliterations of language. Queneau was able to go even further: he wrote 10 sonnets whose lines could be interchanged as the reader wished. This gave exactly *A Hundred Thousand Billion Poems!*

LÉVI-STRAUSS: We have mentioned the word 'structure' a number of times, but at that time I was still not a structuralist. Or if I was, I hadn't yet realised. I remember a moment of lucidity at the end of 1939, although I am unsure as to whether it was not in fact a subsequent elaboration. The memory is like a box full of old photographs. As a soldier, I had been responsible for censoring telegrams, but I found the job so boring that I asked for them to assign me another, which they did. I don't know how they came to cast me off, together with three or four others, at the Maginot Line, on which we spent the whole winter waiting in vain for the possible arrival of the British. On one of my walks – it was our only occupation – I was left looking at a dandelion. The fact that it was a dandelion and not a rose made me think that the story is not completely invented. The fact is that I was awestruck by a humble dandelion, and I suddenly realised that everything that could be said about it was by comparison

with exterior elements. If we forgot about the rest, it could only be said that the dandelion existed. There was a set of relationships that formed a structure in reality, without which nothing would exist.

WEIL: The structure that Jakobson had found in linguistics…

LÉVI-STRAUSS: Meeting Roman Jakobson was a one-way trip, one of those experiences that nobody escapes from unscathed. We arrived in New York at the same time and met in the *École libre des hautes études*, the French university in exile. If in my case, my departure had been caused by the laws of the Vichy government, in the case of Jakobson it was the October Revolution. He didn't like to talk about it – somebody has written that he possessed a "nobleness of science that should not be disturbed by biographic contingencies" – but I know that the political outlook pushed him to accelerate his education so as to be intellectually prepared. As soon as was possible, he set off to Czechoslovakia as an interpreter for the Red Cross, where he founded the Prague Circle in the company of the Russian prince Nikolay Trubetskoy. Together they laid the foundations of modern phonology, the great achievement of which was to transform what is continuous in nature – each speaker pronounces sounds in a different way – into discrete units of recognisable phonemes that form a closed set. Imagine if it were possible to do the same with semantics!

For a number of years, Jakobson attended my classes, and I attended his. Afterwards we would talk for a long time in one of the nearby coffee shops. He had that Greek passion for conversation at the banquet. He was a man who preferred dialogue to monologue, even when it came to research, giving rise to many instances of collaboration. The two of us, for example co-authored a commentary to the poem *The Cats* in which Baudelaire contrasts the image of the 'ardent lover' with the 'austere scholar', united only by their love of cats. I think that is the only occasion on which an anthropology journal has published an analysis of a French poem from the 19th century. Jakobson had the gift of arousing the passions of those he spoke to, whom he always addressed as equals for anything that he would explain to them. It didn't matter if the topic of the day was the art of the Russian formalists or the relationship between the genetic code and the linguistic code. With him, one always felt, as Isaiah Berlin remarked on one occasion, on an ascending curve – more sensitive, more interesting than what it really was. I wonder where Jakobson is now. Perhaps he should join us!

WEIL: Perhaps we would fight to see who knows the most languages.

LÉVI-STRAUSS: You would find that difficult, Mr Weil, he knows six or seven. I

think you would enjoy each other's company. In fact, it was Jakobson who encouraged me to write *The Elementary Structures of Kinship* when I finished a course that I had based on the material in the winter of 1942. It was then that he proposed I do the same thing with ethnology that he and his collaborators had done in linguistics. However, it seems that, in order to go on, you will need to refresh my memory of the group theory that you know so well.

Chapter 3

A History of Groups

Mathematics is just one
history of groups.
H. Poincaré

WEIL: Take a seat, Mr Lévi-Strauss.

LÉVI-STRAUSS: Are you going to explain what a group is?

WEIL: I'll try. I would like to start with an extremely simple example, in which we shall see how a large part of the basic constructions of group theory emerge. I'm going to ask you to imagine an equilateral triangle; I hope you remember this is a triangle with three equal sides. I'm interested in the operations that do not change the position of the shape, such that a person who saw the triangles before and after one of these transformations would be unable to distinguish them; for this reason, we say they leave the triangle *invariant*.

LÉVI-STRAUSS: Sorry to interrupt, Mr Weil; there's something I don't understand. If the shape doesn't change when these transformations are applied, how do we know if they have been applied or not? Triangles don't have memories!

WEIL: A good question; I was just coming to that. The trick consists of numbering the vertices. Although the triangle remains the same, the operations change the position of each number and thus leave 'footprints' that we can interpret; this is a convention. The first operation we shall consider is a 120° anticlockwise rotation with respect to the centre of the triangle.

We shall call this operation R. As I said, the difference between having applied R or not is imperceptible, but if we decided, for example, to order the vertices of the triangle starting with the top one and then continuing in an anticlockwise direction, we could say that R transforms the first vertex into the third, the second into the first and the third into the second. We can see this more easily in a drawing:
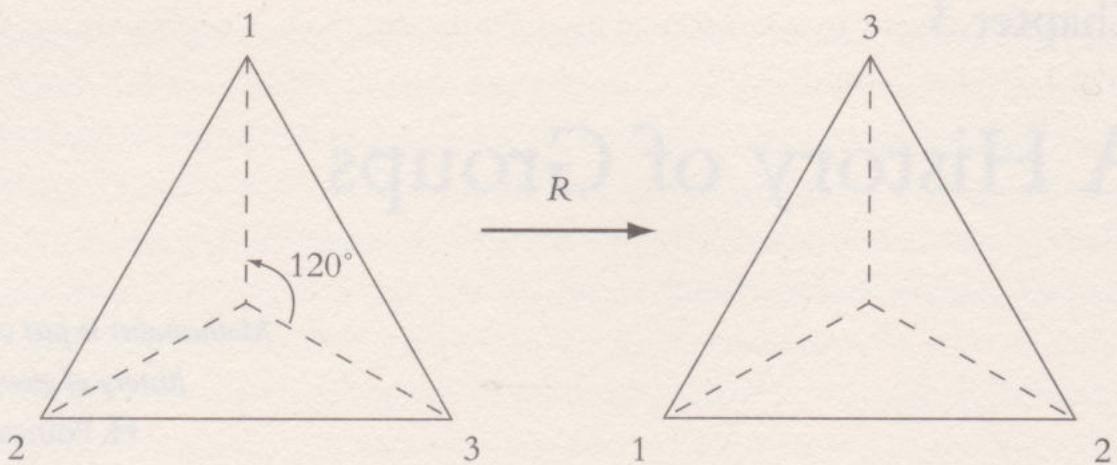
It's easy to apply the rotation R.

Can you see? The triangle is unchanged, however 1-2-3 has become 3-2-1.

R is not the only operation that leaves the figure invariant. Let us now imagine a symmetry with respect to one of the axes that cross the triangle. To conform to the type of transformations we are looking for, we must choose the axis correctly, since there are symmetries that change the position of the shape:
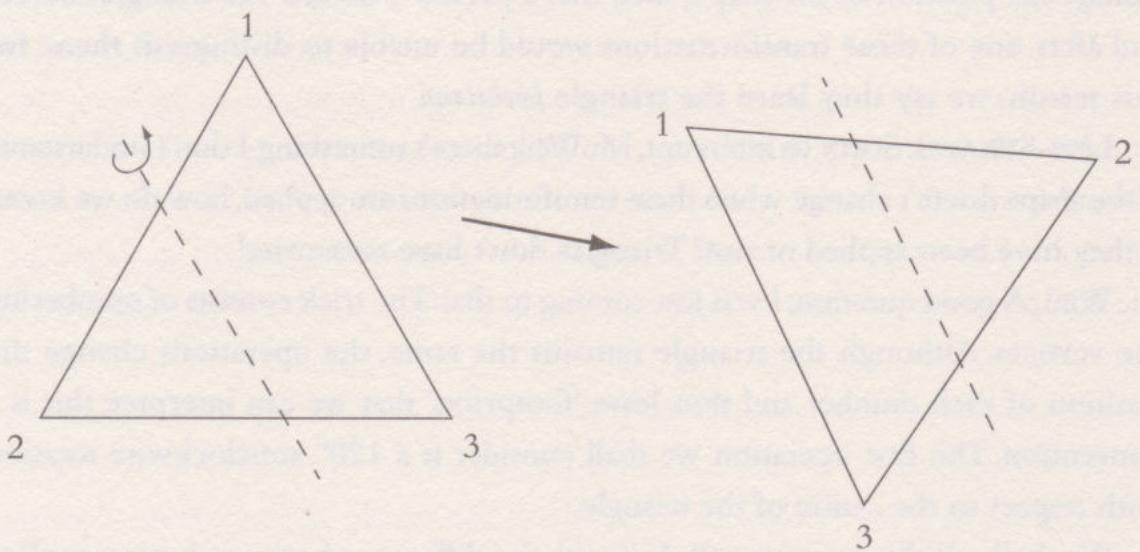
A symmetry that does not leave the triangle invariant.

The triangle can only be invariant when the axis of symmetry passes through the centre and one of the vertices, such as the first. Let us call this operation S. If before we used R for rotation, now we use S for symmetry. Using the same scheme that allowed us to understand the rotation R we can see how the vertices change if we apply the operation S. The first remains unchanged since it lies on the axis, whereas

S switches the other two. The second becomes the third and vice versa. Hence, the order 1-2-3 has become 1-3-2:
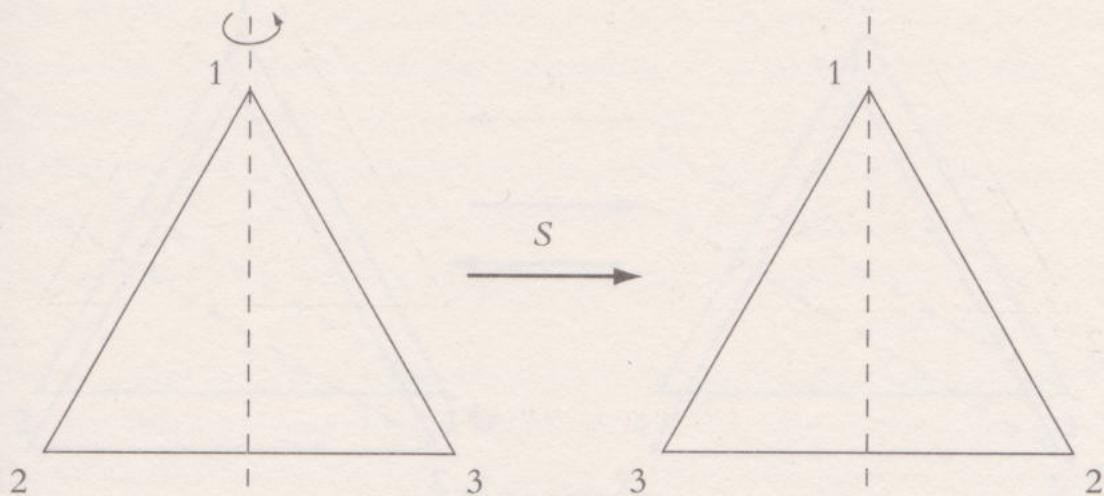

The result of applying the symmetry S.

We now have the operations *R* and *S*. What would you do with them?

LÉVI-STRAUSS: Good question… I don't know… Apply the first and then the other?

WEIL: Exactly! The fundamental property of these operations is that, given two, it is possible to obtain a third via their *composition*. I'm going to write *SR* to refer to the result of first applying the rotation *R* and then the symmetry *S*. To allow us to read from left to right, it would be more logical to use *RS*, since *R* is the first operation. However, the notation *SR* has its advantages. Trust me, and let us calculate the composition:
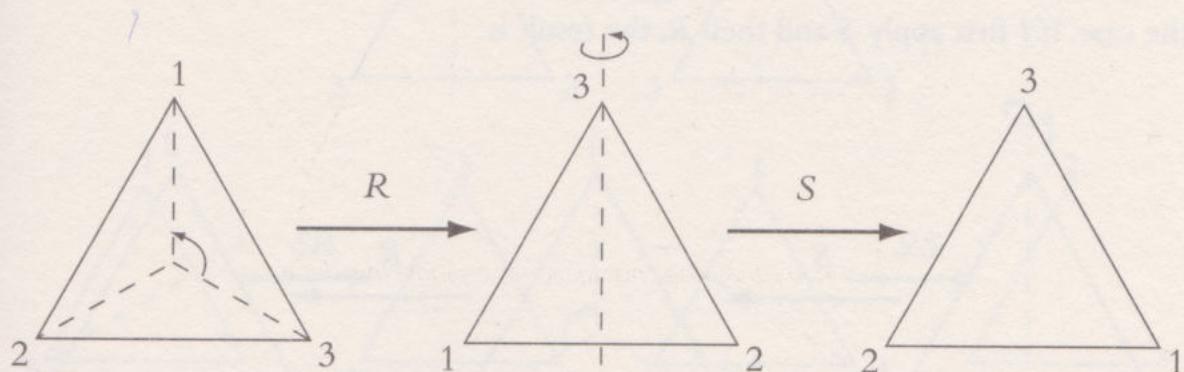
Composition of the operations R and S.

The drawing shows that the operation *SR* fixes the second vertex and switches the other two. The order 1-2-3 is thus sent to 3-2-1. Note that we could have

obtained the same result using the symmetry whose axis passes through the second vertex. In fact, the two operations are the same:
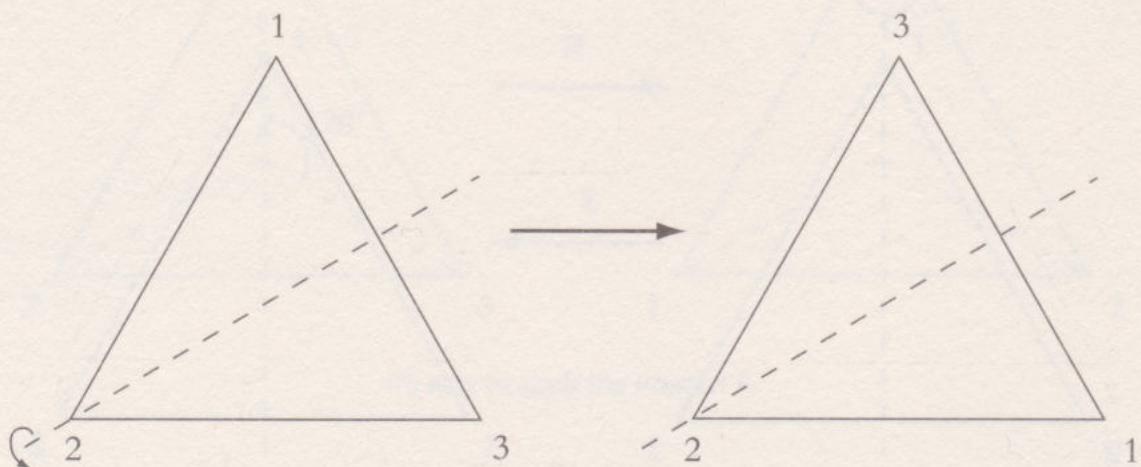

The composition SR is a symmetry.

Let us now calculate *RS*, or rather, the result of first applying *S* and then *R*. As before, it suffices to see what happens to the vertices.

LÉVI-STRAUSS: Wait a moment! The order of the factors does not change the product.

WEIL: Ah, infancy, the paradise of certainties! How difficult it is to change what we have been taught from an early age. "The order of the factors does not alter the product" only refers to the multiplication of numbers – three times seven is the same as seven times three. However, there is no reason why other operations, such as the composition of operations that leave a shape invariant, should comply with this principle, Mr Lévi-Strauss. In fact, here we have an example in which this is not the case. If I first apply *S* and then *R*, the result is:


Composition of the operations S and R.
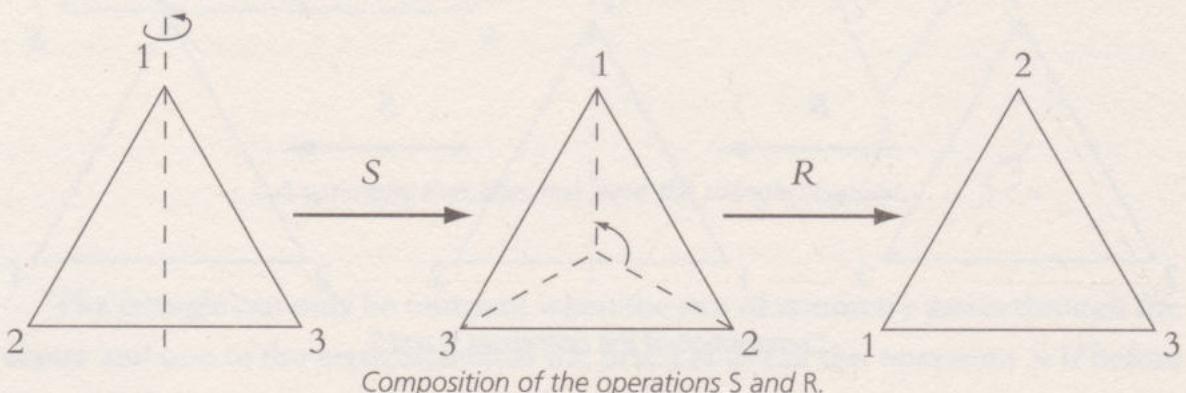
The final configuration is 2-1-3 and hence the results of the operations *SR* and *RS* are different.

LÉVI-STRAUSS: But *RS* is also a symmetry…
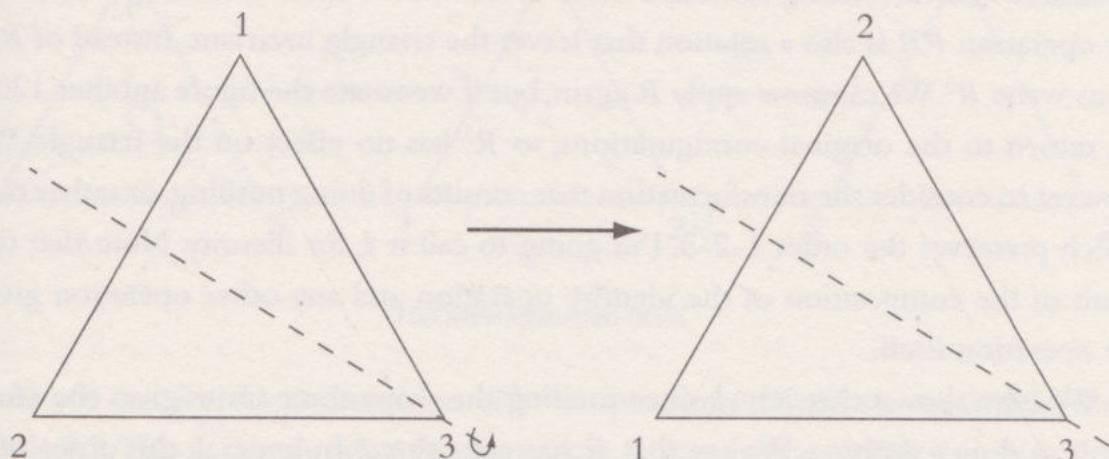
RS is a symmetry.

WEIL: Yes, its axis passes through the third vertex. A while ago I explained to you that, for a symmetry to leave the triangle invariant, its axis must contain the centre and one of the vertices, do you remember? Well, based on *R* and *S* we have recovered them all. If the axis passed through the second vertex, the symmetry would be *SR*, and if it passed through the third, it would be *RS*. Adding *S* itself, which is the symmetry with respect to the first vertex, completes the list: *S*, *SR* and *RS* are all the symmetries that leave the triangle invariant.
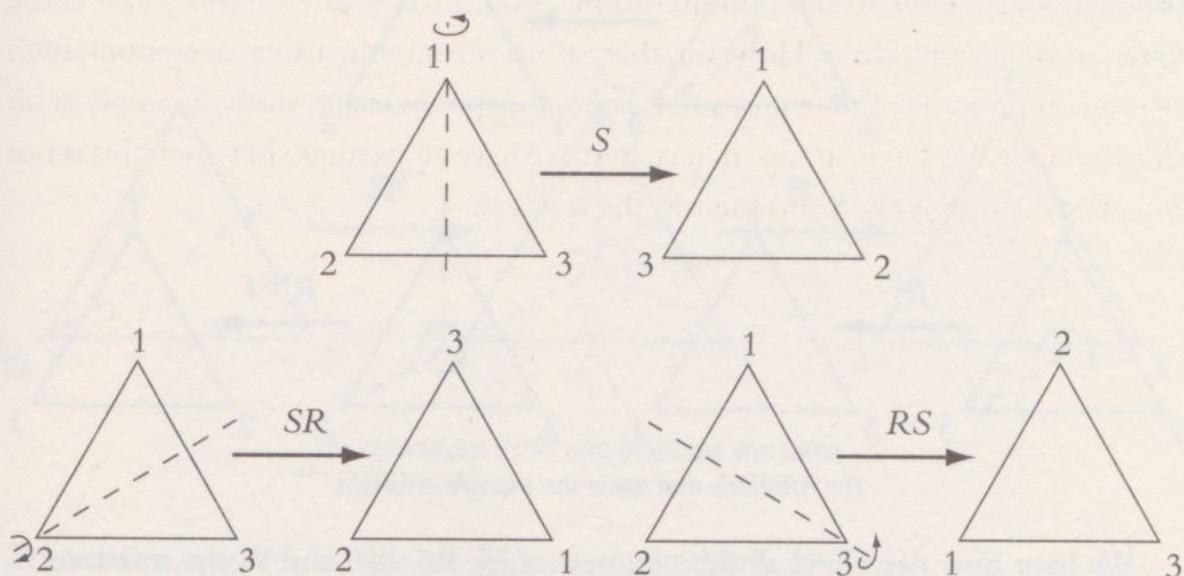

The symmetries that leave the triangle invariant.

LÉVI-STRAUSS: Excuse me, Mr Weil, in order to be able to compose two transformations, is it necessary for them to be different?

WEIL: Absolutely not. There is nothing to stop us repeatedly applying the same operation. Hence, rotating the shape twice by 120° is the same as rotating it by 240°, the operation RR is also a rotation that leaves the triangle invariant. Instead of RR let us write R^2. We can now apply R again, but if we rotate the figure another 120°, we return to the original configurations, so R^3 has no effect on the triangle. We have yet to consider the transformation that consists of doing nothing, or rather that which preserves the order 1-2-3. I'm going to call it I, for identity. Note that the result of the composition of the identity operation and any other operation gives the operation itself.

We have shown that $R^3 = I$, since rotating the shape three times gives the same result as doing nothing. We say that R has *order* three. In general, the order of a transformation is the number of times it must be applied to obtain the identity. For example, S has order two, since repeating the symmetry twice gives the original triangle. We have already seen that the symmetries of the triangle are S, RS and SR. Which rotations leave the shape invariant? Note that a rotation only complies with this property if the angle is a multiple of 120°. Hence, all the rotations are R, R^2 and $R^3 = I$.
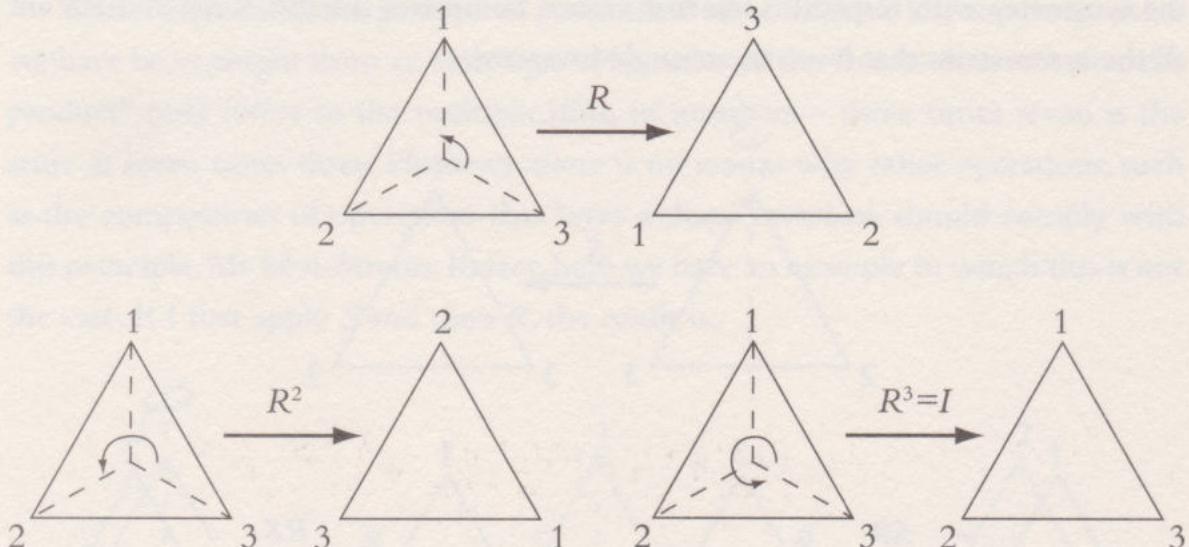
The rotations that leave the triangle invariant.

We have now described all the symmetries (S, RS, SR) and all the rotations (I, R, R^2). A theorem states that any other operation that leaves the triangle invariant can be obtained from a composition of symmetries and rotations. We know how R and S operate but we have not yet obtained the result of first applying the rotation R and then the symmetry RS:
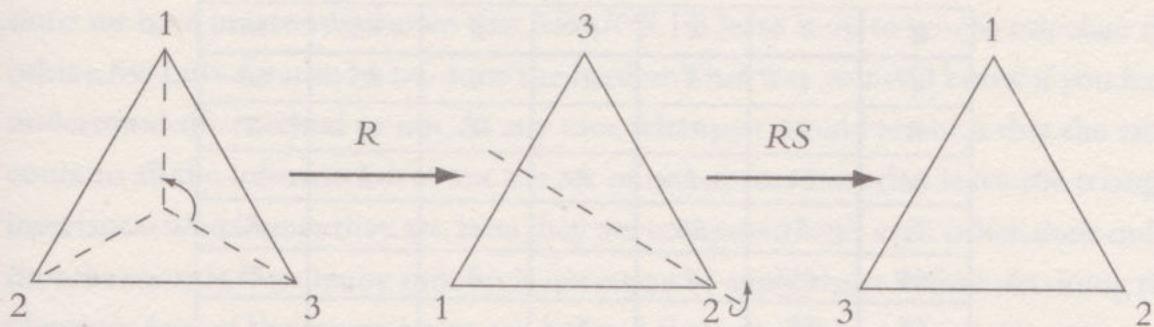
The transformation (RS)R.

As you can see, the composition of both operations transforms the order 1-2-3 into 1-3-2. This is exactly what the symmetry S does, hence $(RS)R = S$.

LÉVI-STRAUSS: What do the brackets mean?

WEIL: It is a way of indicating how the operations are composed. Writing RSR, in which the three operations appear in a row, is ambiguous. Does this mean that the operation R should be applied first, followed by the operation RS, as we have just seen, or do I start with RS and then R? In the former case, we write $(RS)R$, and in the latter, $R(SR)$. The result can be different. Consider, for example, the subtraction of natural numbers. Writing $7-(5-3)=7-2=5$ is not the same as writing $(7-5)-3=2-3=-1$. In this case it is essential to know where to put the brackets. However, we are lucky the operations $(RS)R$ and $R(SR)$ are the same:
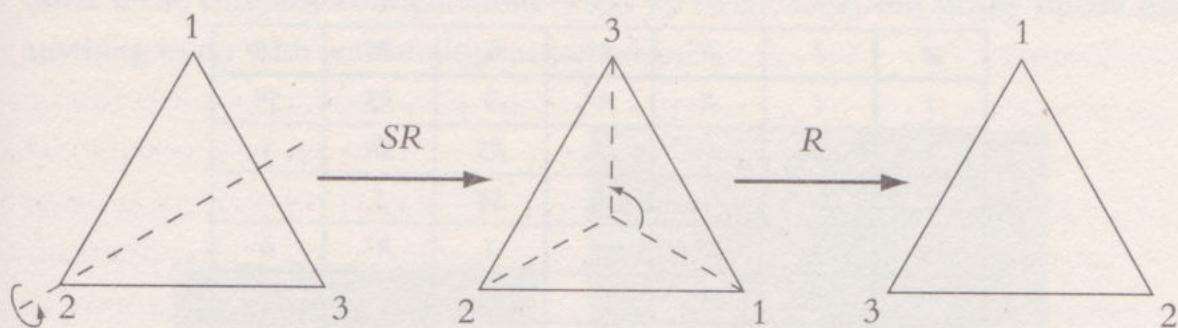
The operations R(SR) and (RS)R are the same.

LÉVI-STRAUSS: You've lost me with so much information!

WEIL: That doesn't surprise me. I propose that we order the information in a 'multiplication table', like the ones used at school, in which each box indicates the result of the composition of the operations in the corresponding row and column, starting with the column (as shown by the arrow):

↙	I	R	R²	S	RS	SR
I	I	R	R²	S	RS	SR
R	R	R²	I	RS		S
R²	R²	I	R		S	
S	S	SR		I		R
RS	RS	S		R		R²
SR	SR		S			I

For the time being, I have only used what we already knew – that the composition with the identity does not alter the transformations, that $RSR=S$ and that $R^3=S^2=I$. This allows us, for example, to calculate $SRSR$. As we can arrange the parenthesis however we like, we have $SRSR=S(RSR)$. According to the previous calculation, $RSR=S$, and $SRSR=SS=S^2$, which is the identity because the symmetry S has order two. Hence, $SRSR=I$. However, the table is not yet complete. One of the missing compositions is SRS. To deduce its value, we will recall that $RSR=S$. The two operations are still the same if I compose them on both sides with R^2, in other words: $R^2RSR=R^2S$. However, we know that $R^2R=R^3=I$, hence the expression is simplified to $SR=R^2S$. This was another of the compositions we didn't know how to calculate! We can still multiply both sides by S, this time on the right. Hence we obtain $SRS=R^2S^2$, however since $S^2=I$, we can conclude that $SRS=R^2$. Let's add these new calculations to the table:

↙	I	R	R²	S	RS	SR
I	I	R	R²	S	RS	SR
R	R	R²	I	RS	SR	S
R²	R²	I	R	SR	S	
S	S	SR		I	R²	R
RS	RS	S		R		R²
SR	SR	·	S	R²		I

We still haven't finished. We're missing the compositions R^2SR, SR^2, RSR^2, $RSRS$ and SR^2S, which can be deduced from the previous ones using the same tricks, try it! For example, R^2SR is the same as $R(RSR)$. But we know that $RSR=S$, hence $R^2SR=RS$. Similarly:

$$SR^2=(SR)R=(R^2S)R=R(RSR)=RS,$$

since we have previously shown that $SR=R^2S$. I'll leave it up to you to calculate the others, Mr Lévi-Strauss; I have done the hardest. That way you will know if you have understood the method or not. At any rate, what you should retain is that the table contains all the information about the set of transformations that leave the triangle invariant – which ones they are, how they are composed with each other, their order (in other words, how many times it is necessary to apply them before obtaining the identity). Any of these properties can be read from the table.

⬋	I	R	R²	S	RS	SR
I	I	R	R²	S	RS	SR
R	R	R²	I	RS	SR	S
R²	R²	I	R	SR	S	RS
S	S	SR	RS	I	R²	R
RS	RS	S	SR	R	I	R²
SR	SR	RS	S	R²	R	I

Table of the transformations for the triangle.

LÉVI-STRAUSS: Perhaps I'm being stupid, Mr Weil, but while you were completing the table, I remembered Dürer's *Melencolia I*, that beautiful image in which a winged figure drowns itself in geometric reflections. As you know, a magic square appears in the engraving in which all the rows and columns – as well as the diagonals and other more complex configurations – add up to 34. Does this magic square have anything to do with your multiplication tables?
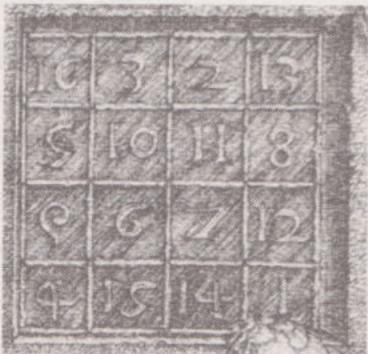
WEIL: Almost nothing, I fear. The most important difference between the two is that, in the multiplication table for a group, all the rows and columns contain the same elements, whereas in a magic square they are never repeated. The first row of Dürer's square contains the numbers 16, 3, 2 and 13, and the second, the numbers 9, 10, 11 and 8. The point is that they are different. Our table is similar to a *Latin square*. You may not have heard of these, Mr Lévi-Strauss; they are not as popular as magic squares. A Latin square is an arrangement of symbols that appear precisely once in each row and column. For example:

1	2	3
2	3	1
3	1	2

One of the things I shall explain to you later is that the multiplication table for a group with a finite number of elements is always a Latin square.

LÉVI-STRAUSS: Okay, let's return to groups.

WEIL: I wanted to give a detailed example of the transformations of the triangle so that we can now extract the underlying structure together. If there is one person to whom I do not need to explain what I mean by the 'underlying structure', it is you, Mr Lévi-Strauss. It is a matter of getting rid of everything that is anecdotal so that we are only left with what can be generalised. Without going into any more detail, let us begin by getting rid of the triangle. Remember that our object of study was not the shape in its own right, but a series of operations carried out on it, which we have called R, S… Let us substitute them for an arbitrary collection of elements (finite or infinite), which we shall represent using the letter G. In the case of the transformations of the triangle, the richness of the example comes from the possibility of composing two operations to obtain a third with the same properties. Let us require the same again. For each pair of elements in G there must be a way of obtaining another that remains part of G. Previously, we represented this composition by juxtaposing the two terms. Now we can introduce a new symbol, such as $*$, to indicate how two elements of G define a third. Hence, $a * b$ will be the result of 'multiplying' a and b according to the operation for the group.

We could stop here, but the structure is not sufficiently restrictive to guarantee that the objects that possess it are of interest. If I give you, for example, a set made up of just three letters, for example $G = \{x, y, z\}$, there are 19,683 different ways of

defining an operation that associates each pair of elements to a third. Too many! It is necessary for ∗ to satisfy certain properties. When it comes to importing these properties, we shall find inspiration once again in the transformations of the triangle. If you recall, we have the identity I, which does not alter any of the other operations when composed with them. Similarly, we would like to have an *identity element*, e, such that the equalities $a ∗ e = e ∗ a = a$ hold for any element a of G. For the set $\{x, y, z\}$, this reduces the number of possible operations to 81; you can already see the difference. The freedom to arrange brackets has also been essential when it comes to carrying out calculations. Hence, for operations involving three elements, we require $(a ∗ b) ∗ c$ to be the same as $a ∗ (b ∗ c)$. The operation is said to be *associative*.

It would not be far-fetched to say that a group is a set with an associative operation that has an identity element. In fact, such a structure exists and is called a *monoid*. It was Bourbaki who introduced that term. This could well have been the definition of a group, but the transformations of the triangle have another property that we are interested in generalising – they are reversible, in the sense that once one has been applied, there is always another that returns the triangle to the original position. This is called the *inverse* operation. Imagine we apply the rotation R. If we then apply R^2, we obtain $R^2 R = R^3 = I$, so R^2 is the inverse transformation of R. On other occasions, an operation might be its own inverse. This is the case, for example, with the symmetries S, RS and SR. Returning to our abstract group, the existence of an inverse is symbolically represented by the fact that, given an element a of G, there is always another element b such that $a ∗ b$ and $b ∗ a$ give the identity element. It is often written as a^{-1} instead of b. That is a group. We will see later on that there is only one way of defining a group law for the set $\{x, y, z\}$.

Definition. A *group* is a set G with a composition ∗ which, for each pair of elements a and b in G, associates another element $a ∗ b$ in G, such that the following properties hold:

a) Composition ∗ is *associative*, in other words, the equality $(a ∗ b) ∗ c = a ∗ (b ∗ c)$ holds for any a, b and c in G.

b) There is an *identity element* e in G such that the equalities $a ∗ e = e ∗ a = a$ hold for any choice of a in G.

c) Given any a in G, it is possible to find an element b in G that satisfies the relationships $a ∗ b = b ∗ a = e$.

The first operation that one can imagine is the sum of the natural numbers 0, 1, 2, 3… It is clear that the operation is associative and that zero is the neutral element, but for it to be a group there must also be an inverse for each number. To achieve this, we add the negative numbers: -1 is the inverse of 1 since $1+(-1)=(-1)+1=0$; similarly, -2 is the inverse of 2, and so on. This gives the group of integers, represented using the letter $\mathbb{Z}$ and with an infinite number of elements. If however, instead of taking the sum, we take the operation of subtraction, we would not have a group, since, as we have seen, it is not an associative operation.

LÉVI-STRAUSS: Returning to the definition of a group, if I give you two arbitrary elements a and b, is it not also the case that $a*b$ and $b*a$ are the same?

WEIL: Not always. That's the reason why, when devising the properties b) and c) I need to write the composition in both directions; it is not sufficient to impose $a*e$ is equal to e, because there is no up-front reason for $e*a$ to be the same as $a*e$. However, if we impose the condition that for two arbitrary elements of the group $a*b=b*a$, we exclude some extremely interesting examples. You have already seen that switching the order of R and S changes the result, so the transformations of the triangle would not form a group with this stricter definition. Of course, the fact that $a*b$ and $b*a$ are not, generally speaking, the same does not prevent the existence of elements a and b such that $a*b=b*a$. In that case, we say that a and b commute. You will recall that many of the rules for marriage in your tribes translate into the commutativity of two elements! There are even groups in which all the elements are commutative. These are *commutative* or *abelian* groups.

LÉVI-STRAUSS: Commutative I can understand, but why abelian?

WEIL: The name is in honour of the Norwegian mathematician Niels Henrik Abel (1802–1829), who used early group theory to prove it was impossible to solve almost all fifth-degree equations using elementary methods. It was Camille Jordan who gave them the name 'commutative' in his *Treatise on Substitutions and Algebraic Equations* in 1870. Jordan had the brilliant idea of turning what could have continued to be a name into an adjective. This is also a characteristic of the naming conventions introduced by Bourbaki. We did not speak of Riemann geometry or Artin rings, but *Riemannian* geometry and *Artinian* rings. By removing the explicit reference to the name of the creator, the concept allowed new intuitions to unfold.

LÉVI-STRAUSS: What about Évariste Galois? Was not he the one who invented groups? Somebody told me the story of the night before the duel…

WEIL: Oh how you all love that story! I have often had to hear that, since he was going to die the following day, Galois received the inspiration required to

develop his entire theory in the space of one night. In fact, it was Galois who used the word 'group' for the first time in a series of articles that must rank among the most beautiful pages in the history of humankind; it is difficult to know how far his influence extends. However, the groups being studied by Galois had a different aspect from the ones I have been telling you about. He was interested in *permutation groups*. Given a set of *n* elements, such as the natural numbers from 1 to *n*, a permutation is a new way of ordering them. Indeed, it is possible to define a group operation for the set of permutations. Imagine we select the following permutations

$$\sigma_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{bmatrix} \text{ and } \sigma_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{bmatrix}$$

from the set of five elements $\{1, 2, 3, 4, 5\}$. This is a way of indicating that, after the permutation σ_1, the set becomes $\{2, 5, 3, 1, 4\}$, and after applying σ_2, it becomes $\{3, 4, 5, 1, 2\}$. As you can see, below each number of the initial configuration is the number that replaces it after the permutations. To provide these operations with a group structure, it is necessary to define a method for their composition. I'll explain how to do this. To determine the value of $\sigma_1 * \sigma_2$, I must first consider the number that appears below the element 1 in σ_2; which is 3. I then look at which number corresponds to 3 in the permutation σ_1; which is 3. Hence I say that in the composition $\sigma_1 * \sigma_2$, the 1 is sent to 3. Let us now see what happens with 2: σ_2 sends it to 4, and σ_1 sends 4 to 1, hence in the composition $\sigma_1 * \sigma_2$, the number 2 is sent to 1. If we continue this procedure, in the end we have

$$\sigma_1 * \sigma_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{bmatrix},$$

and this method for the composition of permutations satisfies all the properties for the definition of a group. This gives us the *symmetric group* S_n, where *n* is the number of elements of the set of permutations.

LÉVI-STRAUSS: Where do these groups appear?

WEIL: Everywhere! In fact, there is a theorem that states that any finite group can be found inside a symmetric group; all that is necessary is to correctly choose *n*. We

have already worked with a symmetric group, although you may not have realised it. Can you remember how we distinguished the transformations of the triangle? We numbered the vertices and saw how they changed as the operations were applied. But this means that a transformation of the triangle is nothing more than a way of permuting the numbers 1, 2 and 3. To associate a permutation with each operation, it is necessary to consider the spaces occupied by the vertices after having applied it. For example, after the rotation R, the first vertex occupies the position held by the second, meaning that the associated permutation sends 1 to 2. Similarly, the vertices 2 and 3 can now be found in the positions for 3 and 1, respectively, meaning that the permutation sends 3 to 2, and 1 to 3. Hence, the rotation R contains the same information as

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}.$$

Repeating this process for each of the transformations, we obtain the following table of correspondences:

$$I \leftrightarrow \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \quad R \leftrightarrow \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \quad R^2 \leftrightarrow \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

$$S \leftrightarrow \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \quad SR \leftrightarrow \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \quad RS \leftrightarrow \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

Furthermore, note that composing the permutations

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix},$$

which, as we have just seen, represent the elements R and S respectively, results in the following permutation

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix},$$

which is associated with RS. The correspondence is perfect! From the point of view of the structure, the group of transformations that leaves the triangle invariant is identical to the symmetry group S_3. We say these are *isomorphic*. In general, two groups

G and H are isomorphic if there is a function f that sends each element of G to an element of H, such that the following three properties hold: 1) different elements have different images; 2) all the elements of H are images of an element of G using f, and 3) f respects the group operation, or in other words: given g_1 and g_2 in G, the result of first carrying out the operation on g_1 and g_2 in G and then calculating the image of the product is the same as calculating $f(g_1)$ and $f(g_2)$, and then carrying out the operation according to the law for group H.[1]

LÉVI-STRAUSS: Excellent, where to now?

WEIL: Now that we have extracted the axioms that define the group structure, we can use them to prove theorems that will hold for any situation that satisfies the conditions – in this instance, for our group of transformations of the triangle! Let us consider some simple examples. We shall begin with the identity elements. Point b) in the definition of a group states that there is an element e with the property that $a*e=e*a=a$ for any a, but it says nothing about how many elements of the group share this property. There may well be more than one. However, point c) of the definition tacitly assumes that the identity element is unique, since if this were not the case, it would be necessary to specify which of the identity elements we want to coincide with the composition of a term and its inverse. To be fully rigorous, as soon as we have stated the axiom b) we must have shown that the identity element is unique. We shall do so now. To do so, imagine that there are two identity elements e_1 and e_2. Our aim is to show that $e_1=e_2$. Let us consider the product e_1*e_2. On the one hand, e_1 is an identity element in the sense that it does not change any other element when it appears as an operator on the left. Hence, $e_1*e_2=e_2$. On the other hand, e_2 is also an identity element, meaning that after multiplying an element by e_2 on the right, it does not change. Hence, $e_1*e_2=e_1$. We have shown that e_1*e_2 is the same as, e_1 and e_2, hence e_1 and e_2 must be the same!

There can be only one identity element. In a group, there is only one element with the property $a*e=e*a=a$ for all a in G.

LÉVI-STRAUSS: Are inverses also unique?

WEIL: Yes! Just like before, imagine there are two elements b_1 and b_2 such that

---

1 The concept of the isomorphism of groups is covered in detail at the start of the Appendix.

$a * b_1 = b_1 * a = e$ and $a * b_2 = b_2 * a = e$. Specifically, we have $a * b_1 = a * b_2$ because both terms are the same as e. The equality must continue to hold if we multiply both sides by the element b_1, or rather, we have $b_1 * a * b_1 = b_1 * a * b_2$. Remember that, when it comes to taking the product of three elements, I can arrange the brackets however I want. Hence,

$$b_1 * a * b_1 = (b_1 * a) * b_1 = e * b_1 = b_1$$

since $b_1 * a = e$, and e is the identity element. Similarly,

$$b_1 * a * b_2 = (b_1 * a) * b_2 = e * b_2 = b_2.$$

Since both expressions are the same, we have $b_1 = b_2$. Thanks to this property, I can refer to the element b as the *inverse* of a and write $b = a^{-1}$.

I'm very pleased that you asked me that question, Mr Lévi-Strauss, because in answering it, I have made use of a proposition that will be extremely useful to us in the future. Note that, starting from the equality $a * b_1 = a * b_2$, we have deduced that $b_1 = b_2$. This is a general property of groups – if the result of multiplying two elements by a third common element of the same order is the same, then the initial elements are the same:

> **Property of elimination.** If for a group G we know that the equalities $a * b = a * c$ or $b * a = c * a$ hold, then $b = c$.

LÉVI-STRAUSS: How can we prove something like this?

WEIL: It's quite simple. All we need to do is copy what we have already done. Imagine that we have the equality $a * b = a * c$. Axiom c) of group theory states the existence of an inverse element for a, which is also unique. Let us call it a^{-1}. The equality still holds if I multiply the two terms of the equation by a^{-1} on the left. Hence: $a^{-1} * a * b = a^{-1} * a * c$. Having reached this point, I can use associativity to group a with its inverse.

Since I know that $a^{-1} * a$ is equal to e, the identity element, I can deduce on the one hand that $a^{-1} * a * b = (a^{-1} * a) * b = e * b = b$ and, on the other, that $a^{-1} * a * c = (a^{-1} * a) * c = e * c = c$, hence there is no other alternative than $b = c$. If instead of the equality $a * b = a * c$, we have $b * a = c * a$, it is enough to repeat the procedure, multiplying on the right instead of the left.

LÉVI-STRAUSS: And what use is this property?

WEIL: Well, for example, to show that the multiplication table of a finite group is a Latin square. Remember that this means that all the elements of the group appear in every row and column. Let us call them $a_1, a_2 \ldots a_n$. I'm going to show you the proof for the second row of the table; the method is exactly the same for any other column. Which elements appear in the second row? They are the ones obtained by multiplying a_2 on the left by all the elements of the group, or rather: $a_2 * a_1, a_2 * a_2,$ $a_2 * a_3 \ldots$ up to $a_2 * a_n$. Imagine that two of the terms in this list are the same, or in other words there are two subscript indexes j and k such that $a_2 * a_j = a_2 * a_k$. Since a_2 appears on both sides of the formula, we could apply the property of elimination to conclude that $a_j = a_k$. There are no two elements the same in that row! However, if the group is made up of n and n must appear in a row without being repeated, it is necessary for it to contain all the elements of the group! Do you understand?

LÉVI-STRAUSS: And the same holds for the rows of the table, by changing the direction of the multiplication…

WEIL: Your progress surprises me, Mr Lévi-Strauss. I think you are now ready to be introduced to new groups. Remember that I told you a while ago that it was only possible to define a group operation for a set with three elements? I'm now going to explain why, but before studying the case for three elements, it is necessary to understand what happens when a group has order one and two. Did I explain to you what the *order* of a group means? I don't think so. When a group is finite, the term order refers to the number of elements.

LÉVI-STRAUSS: Did we not use the word for something else?

WEIL: Yes and no. When we studied the example of transformations of the triangle, I said that R was of order three, since rotating the shape three times by 120° is the same as doing nothing. In general, an element was of order n if the result of operating on itself n times gave the identity. Perhaps it seems that this definition has nothing to do with the previous one, but I will show you how they are related.

Given an arbitrary element of a group, which we shall call a, I can form the set of the powers of a, in other words, $<a> = \{a, a^2, a^3 \ldots\}$, where, by convention, a^2 is an abbreviation for the notation $a * a$, a^3 means $a * a * a$, etc. Imagine that a has order n according to my first definition, in other words a^n is the neutral element of the group. Hence, the list of powers stops at $a^n = e$ and returns to the start, since $a^{n+1} = a^n * a = e * a = a$, $a^{n+2} = a^2$, and so on. In fact, the set only has n elements: $<a> = \{a, a^2, \ldots, a^n = e\}$. Hence, the order of an element is the order of the group formed by its powers. My new definition, if you like, is more general than the first.

Anyway, that's not what I wanted to tell you. I propose that we handle groups by considering the properties of those with the lowest order. Among the properties for the definition of a group, we included the existence of an identity element, hence a group cannot be empty; it always contains at least the identity element. When it is of order one, there can be no other element, hence $G=\{e\}$. Let us now see what happens with groups of two elements. They must be of the form $G=\{e, a\}$, where e is the neutral element and a is another element that is not e. By definition, $a*e=e*a=a$, and we also know that $e*e=e$, hence to fully determine the group, we only need to know the value of $a^2=a*a$. As this element must also belong to the group, there are just two options: either $a^2=e$ or $a^2=a$. However, we can rule out the latter immediately, since applying the property of elimination to the equality $a^2=a$, gives $a=e$, and we have said that a and e are different. Hence, there is only one group of order two:

↙	e	a
e	e	a
a	a	e

The group of order two.

LÉVI-STRAUSS: There is something I don't understand. What do you mean by there being only one group of order two? You could substitute the element a for anything.

WEIL: But the multiplication table would still be the same. The appearance of the elements does not matter, what matters is how they are related. The dandelion, once again. As appreciable objects, the permutations of the set $\{1, 2, 3\}$ are completely unrelated to the operations that leave the triangle invariant, however we have seen that both can be paired together such that the group operation is respected. From the point of view of the structure, the two groups are indistinguishable, isomorphic. It is as if they were different realisations of the same platonic ideal: the group of order six with the relations shown in the table. Do you understand?

LÉVI-STRAUSS: Then there is only one platonic ideal for a group of order 3?

WEIL: Only one.

LÉVI-STRAUSS: Let me try. A group of order three is made up of e and another two elements a and b, all of which are different: $G=\{e, a, b\}$. The relations that are known are $e*e=e$, $e*a=a*e=a$ and $e*b=b*e=b$. We begin by calculating a^2. Since

it is an element of the group, there are no more than three possibilities: $a^2 = e$, $a^2 = a$ and $a^2 = b$, however once again we can rule out $a^2 = a$ since a would be equal to the identity element by the property of elimination. This leaves two options: $a^2 = e$ and $a^2 = b$. But this means there are two group models of order three.

WEIL: No, your argument is still not quite right. Imagine that $a^2 = e$. Then the table for the group would begin as follows:

↙	e	a	b
e	e	a	b
a	a	e	
b	b		

Earlier, we showed that the multiplication table for a group is a Latin square, meaning that the rows and columns must contain all the elements. In the second row, we have a and e, meaning that the third entry can only be a b. However, this would mean that b is repeated twice in the third column. This table cannot be completed such that all the elements appear in each row and column, meaning that it is not a group table and, hence, the possibility that $a^2 = e$ is excluded.

LÉVI-STRAUSS: Hence, we must have $a^2 = b$. Ingenious! This means we can write the group as $G = \{e, a, a^2\}$. Do you agree?

WEIL: You still need to define the result of the operation a and a^2, or rather, specify the value of a^3. But this is easy, since a^3, which is an element of the group, can only be e, a or a^2. However, if it was equal to one of the last two elements, then, applying the property of elimination once or twice, we could conclude that a is the identity element. Since this is not the case, we are left with $a^3 = e$. All groups of order three are isomorphic:

↙	e	a	a^2
e	e	a	a^2
a	a	a^2	e
a^2	a^2	e	a

This group already arose when we were studying the transformations of the triangle. Carefully observing the multiplication table that we prepared, you can see that the first quadrant is precisely that of the group of order three. Sometimes

within a group there are other smaller groups that are composed of a subset of the elements. These are called *subgroups*.

↙	I	R	R²	S	RS	SR
I	I	R	R²	S	RS	SR
R	R	R²	I	RS	SR	S
R²	R²	I	R	SR	S	RS
S	S	SR	RS	I	R²	R
RS	RS	S	SR	R	I	R²
SR	SR	RS	S	R²	R	I

A subgroup of order three.

Groups made up of powers of the same element – I forgot to mention it before – are called *cyclic*, and the element is called the *generator* of the group. For a given group G, a family of generators is a finite set of elements from the group which can be used to obtain all the others. For example, the rotation R and the symmetry S generate the group of transformations for the triangle. A good way to imagine a cyclic group is to think of a clock that returns to zero every twelve hours. After midday, the hands return to the current position. Just by looking at them, it is impossible to tell whether time has passed or not. If an election ends at nine o'clock at night and the count lasts for four hours, nobody would dream of adding $21 + 4 = 25$ to conclude that the results will be given at 25 o'clock. Instead, they add four hours to reach 24 and then start from the beginning with the remaining hour, to conclude that the winner will be announced at one o'clock in the morning. Just as there are 12 and 24-hour clocks, we could devise a 'clock' with any number of hours, let us call the number n. The base set will be the natural numbers that are less than n, which we shall write in square brackets to indicate that, in fact, each represents many different times at the same time: $[0], [1], [2]…[n-1]$. We would like to say that the operation between two elements of the set is the usual sum, without square brackets, but note that this also raises a problem. Imagine, for example, that n is 5. The previous set now becomes $[0], [1], [2], [3], [4]$. Adding together the elements 3 and 4, gives $3 + 4 = 7$, which does not belong to the set. It is necessary to refine the construction, and to do so, the trick consists of resetting the counter each time we reach 5. For the case of 3 and 4, $3 + 2 = 5$, which means that after starting the new day, there are

still another two units to be added. Hence, we have [3] + [4] = [2]. There are other sums in which the reset is not required, such as 1 + 2 = 3, which is less than 5, hence I know directly that [1] + [2] = [3]. However, [2] + [3] = [0] and [2] + [4] = [1], since I need to subtract 5 once from the result. This gives the table:

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

Given any number *n,* it is possible to show that this modified addition defines a group operation for the set {[0], [1], [2]...[n−1]}. It is the *cyclic group of order n*, or *the group of integers modulo n*, represented by the symbol Z/*n*.

LÉVI-STRAUSS: Enough, Mr Weil. It's time to talk about marriages!

Chapter 4
Algebraic Marriages

> *The hardest thing for a mathematician tackling a*
> *problem from applied mathematics is often*
> *understanding what it is about and translating the*
> *details of the problem into his own language.*
> A. Weil, comments on his complete works

LÉVI-STRAUSS: Now that you have taught me the foundations of group theory, shall we see how to apply it to the study of structures of kinship. What do you think?

WEIL: We'll begin with an extremely simple model, from which we can gradually extract the principles required to solve more general situations. Imagine that a tribe has four different clans, which may – for example – worship different totems or control certain territories. As the structure of the marriages does not depend on the names of the clans, we shall designate them using four letters, A, B, C and D.

LÉVI-STRAUSS: You'll be pleased to know that one of the first things made clear to me by the Nambikwara Indians when I joined their camp was that the use of proper names was forbidden. That's why I had to use symbols in my census of the tribe, the first step to identifying kin relationships. I also used letters to represent clans and numbers to distinguish each of their members. This resulted in an article filled with changes of temperature, in which the cold-hearted way of referring to somebody as A_7 stood side-by-side with comments along the lines of "exuberant woman, always in a good mood" or "vain, self-satisfied, not very intelligent".

WEIL: The Nambikwara… there's a society well prepared for mathematics. Sometimes the hardest part of a problem is choosing the correct notation, in translating it into a language with which we feel comfortable. In this case, once we have distinguished between the four clans of the tribe, the next step is to study the marriages that are permitted $M_1, M_2, M_3 \ldots$ using as many subscript indices as necessary. Note that in order to describe them fully it is sufficient to just specify the

clans to which the man and women belong. For example, M_1 could be the marriage of a man A with a woman B.

LÉVI-STRAUSS: The time has come to impose some restrictions on the types of marriage. First of all, all the individuals of the tribe, regardless of whether they are men or women, must have the right to marry. This means that, given a man and a woman from one of the clans, there must be at least one rule M_i to which they conform. So far, everything seems reasonable. The following hypothesis attempts to scale down a problem that would be intractable in its totality, and is related, as you know, to title of my thesis: *The Elementary Structures of Kinship*. A tribe is 'elementary' if each of its members is assigned one and only one type of marriage, and the process for selecting a spouse is, in this respect, automatic. At the other end of the spectrum, there are societies, such as ours, which we can describe as 'complex', in which each marriage is influenced by a boundless number of factors (psychological, social, economic, etc.).

What is certain is that there are no strictly elementary societies, since all societies allow a certain degree of freedom within the clan specified by the rules of marriage, and nor are their strictly complex societies, since there are always limitations, such as the prohibition of incest. However, the distinction functions well at a theoretical level.

After studying the elementary structures, my idea was to tackle complex societies, beginning with the Crow and Omaha in North America, who can be divided into tens of clans, and whose rules only establish who somebody cannot marry. This would have been the natural continuation of my thesis, but *Tristes tropiques* got in the way. I never found the strength to tackle a problem that was extremely difficult from a mathematical point of view, and in which it would have doubtless been necessary to enlist the help of computers. As the number of clans increased, the combinatorics of the marriages became increasingly similar to that of chess, where the number of possible games, despite being finite, is in practice so large that it might as well be infinite. If, in order to dissect the elementary structures, I had to consult some 7,000 articles and, in spite of all this, still needed to ask for your advice, who knows what I would have had to do to start to understand something about more complex models...

WEIL: Don't worry, Mr Lévi-Strauss: we'll limit ourselves to studying elementary societies. Let us leave the other work to the youngsters. If you wish, before we continue, we'll recall once again that elementary structures are those that satisfy the following hypothesis:

> **Hypothesis 1:** All the members of the tribe can marry and there is just one type of marriage for each.

Note that in such a society, the number of possible marriages is exactly the same as the number of clans into which the tribe is divided. Hence, in our example we would need to describe M_1, M_2, M_3 and M_4. In fact, since all the men are able to marry, there must be at least four rules, one per clan. Imagine there was a fifth. The rule would require the involvement of a man from a certain clan. Since there are four of those, it must be one of the clans that has already appeared, but this means that the selection was not unique! Hence, we have shown that there must be as many types of marriages as there are clans; no more, no less. However, it does not suffice to have four arbitrary rules: M_1, M_2, M_3 and M_4 must not only take into account all the men, but also all the women. One example of this condition being met is the following:

(M_1) man A with woman B

(M_2) man B with woman C

(M_3) man C with woman D

(M_4) man D with woman A
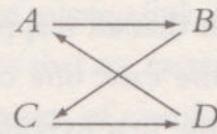
LÉVI-STRAUSS: This is what ethnologists call 'generalised exchange', since none of the pairs of clans exchanges its women: A, for example, marries a woman from B, but the woman from A marries into clan D. Once the types of marriage have been described, it is necessary to explain how inheritance is transmitted. Let's make a new simplifying hypothesis:

> **Hypothesis 2:** The type of marriage for each individual depends solely on their sex and the type of marriage of their parents.

WEIL: This means that there are two functions f and g that define a correspondence between each of the types of marriage M_i and the rules $f(M_i)$ and $g(M_i)$ that govern the marriages of the sons and daughters born of these couples. Therefore, knowledge

of the structures of the kinship of a tribe is reduced to the types of marriage M_i and the functions f and g. Returning to the previous example, imagine that the children of a mother from clan A, B, C or D belong, respectively, to clans B, C, D and A. Let's see how the functions f and g can be calculated. The type of marriage M_1 is between a man A and a woman B, and the inheritance is determined by the mother, hence the children of a marriage M_1 belong to clan C. A man C marries according to the model M_3; we therefore have $f(M_1) = M_3$, while $g(M_1) = M_2$, since the women from clan C obey the second rule. Repeating this process for the remaining marriages gives the following table:

Parents	M_1	M_2	M_3	M_4
Son $f(M_i)$	M_3	M_4	M_1	M_2
Daughter $g(M_i)$	M_2	M_3	M_4	M_1

Note that the effect of the functions f and g consists of permuting the types of marriage, such that all reappear just once in the descendants of the two sexes. If this was not the case, one of these would have disappeared in the following generation, and the first hypothesis would have been violated. Do you remember what I explained to you about the *symmetry group* S_n the last time we spoke, Mr Lévi-Strauss? Indeed, the functions f and g are two permutations of the elements M_1, M_2, M_3 and M_4. By repeatedly composing them, we can reach any corner of the family tree! The complexity of your question about what types of marriage are permitted and what types are not does not matter; with a little patience, we can always reduce it to an algebraic calculation.

Lévi-Strauss: Let's see if this is the case, Mr Weil. Try to investigate if in our tribe women always come from the same clan as their paternal grandmother.

Weil: I thought you were going to test me with something more difficult! Note that in an elementary tribe, the clans to which two members of the same sex belong are the same if and only if their types of marriage are the same. Imagine that the grandparents have married according to M_i. This means that their male children will follow the rule $f(M_i)$, and the women born of the latest marriage will marry in line with $g(f(M_i))$. The type of marriage of the granddaughter is, therefore, the result of first applying f followed by g. Having reached this point, your question translates into the following: does $g(f(M_i))$ coincide with M_i? Or put another way,

does the composition of f and g give the identity? A simple calculation suffices to show that this is not the case: since $f(M_1)$ is M_3 and $g(M_3)$ is equal to M_4, we have $g(f(M_1))=M_4$ and not M_1, as we required. Therefore, if the grandmother belongs to clan B, the granddaughter belongs to clan A. What is certain, however, is that the paternal grandfather and the granddaughter belong to the same clan. Try to prove it!

LÉVI-STRAUSS: Impressive, Mr Weil! These were precisely the calculation techniques I needed in the 1940s to study the prohibition of incest, a problem that had already been studied by the sociologist Émile Durkheim. He was one of the first to show that the prohibition of incest is just the negative form of a broader phenomenon, which is practically universal in nature – *exogamy*. As soon as something is prohibited within a nuclear family, I am obliged to look beyond the clan to satisfy its removal. The reasons are practical, not moral. Many reporters have told us that if you marry your sister, you won't have a brother-in-law. Who would you go out hunting with? Who would you go out with to enjoy yourself? In some senses, my point of view differed from that of Durkheim. What I was really interested in was understanding the transition from nature, governed by universal laws, to culture, in which rules varied from one society to another. Suddenly it occurred to me that the prohibition of incest could represent an intermediary state, a sort of missing link. It is clear that the content of the rule is not universal: there are societies that are extremely strict in this respect and punish relationships we would never dream of classifying as incestuous by the death penalty. I myself would be from one of these illegitimate marriages, since my parents were fifth cousins. Other societies, on the other hand, are so liberal as to allow a man to marry his younger sister, although never an older sister. What is invariable, however, is that there is a rule that prevents people from marrying whoever they like. My hypothesis is that the prohibition of incest articulates the transmission of nature to culture since, being a rule that varies from one society to another, it also approximates a universal law.

WEIL: If I remember correctly, although marriage between cousins is always a border case, the tribes we studied allowed *a man to marry the daughter of the brother of his mother*. Let us see how this possibility translates in terms of the permutations f and g. Instead of directly starting with the man in question, we are going to go back two generations to consider a couple that married according to one of the models M_i. A daughter of this marriage must thus be governed by the rule $g(M_i)$, and a son by $f(M_i)$. These are the mother and brother referred to in the problem. The type of marriage for the man will be $f(g(M_i))$, and the type for the daughter of the brother of the mother will be $g(f(M_i))$. For both to be able to marry, the types of marriage

must be the same: $f(g(M_i)) = g(f(M_i))$. Or put another way, regardless of the type of the initial marriage, the result of applying the function g followed by the function f must be the same as first applying f followed by g. As I explained to you in our last conversation, in this case we say that the elements f and g *commute*. This means that the subgroup S_n that they generate (in other words the set of elements obtained by successively composing f and g) is *abelian*. Abelian groups with two generators are not so difficult to study. I will explain why shortly, but to do so it is necessary to introduce a new concept.

Previously, I gave a handful of examples of the structure of the group. We studied the symmetry group S_3, which appears either as a group of transformations that leave an equilateral triangle invariant or as the permutations of a set made up of three elements. We also discussed cyclic groups $\mathbb{Z}/n$, the elements of which are the natural numbers smaller than n with the same 'modified' sum that we carry out on a clock face made up of n hours. At the time you might have asked me how to construct new groups based on the examples we had considered. I am now going to describe one of the possible procedures. Imagine we have two groups G and H. Since their respective operations have no reason to be the same, I am going to use $*$ to represent the first, and $\bullet$ to represent the second. The underlying set of our new group, which we shall represent by $G \times H$, will be composed of the pairs (g, h), where g is an element of G, and h belongs to H:

$$G \times H = \big\{(g,h) : g \in G,\ h \in H\big\}.$$

We now need to define a group operation. To do so, we apply the laws of G and H coordinate by coordinate. The result of the operation (g_1, h_1) and (g_2, h_2) will thus be $(g_1 * g_2, h_1 \bullet h_2)$. It is easy to check this operation satisfies the three axioms for the definition of a group; I leave it for you as an exercise, Mr Lévi-Strauss. Hence, we have obtained a new group, which we shall call the *direct product* of G and H.

We shall calculate, for example, the direct product of the cyclic group of order two with itself. As you know, the elements of $\mathbb{Z}/2$ are [0] and [1], whose operations follow the rules [0]+[0]=[0], [0]+[1]=[1], [1]+[0]=[1] and [1]+[1]=[0]. Hence, the direct product $\mathbb{Z}/2 \times \mathbb{Z}/2$ is made up of ([0], [0]), ([0], [1]), ([1], [0]) and ([1], [1]). The first of these pairs is the identity element; let us represent it by e. If I denote the others $a = ([0], [1])$, $b = ([1], [0])$ and $c = ([1], [1])$, the table for the group is as follows:

↙	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

This is the *Klein group*, named after the German mathematician Felix Klein (1849–1925), who introduced it in his *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree* in 1884 to study the transformations of the plane that leave the rhombus invariant. Note that it has just four elements, whereas the group for the triangle has six. This is logical, since, in a certain sense, the groups measure the symmetry and a rhombus is less symmetrical than a triangle!
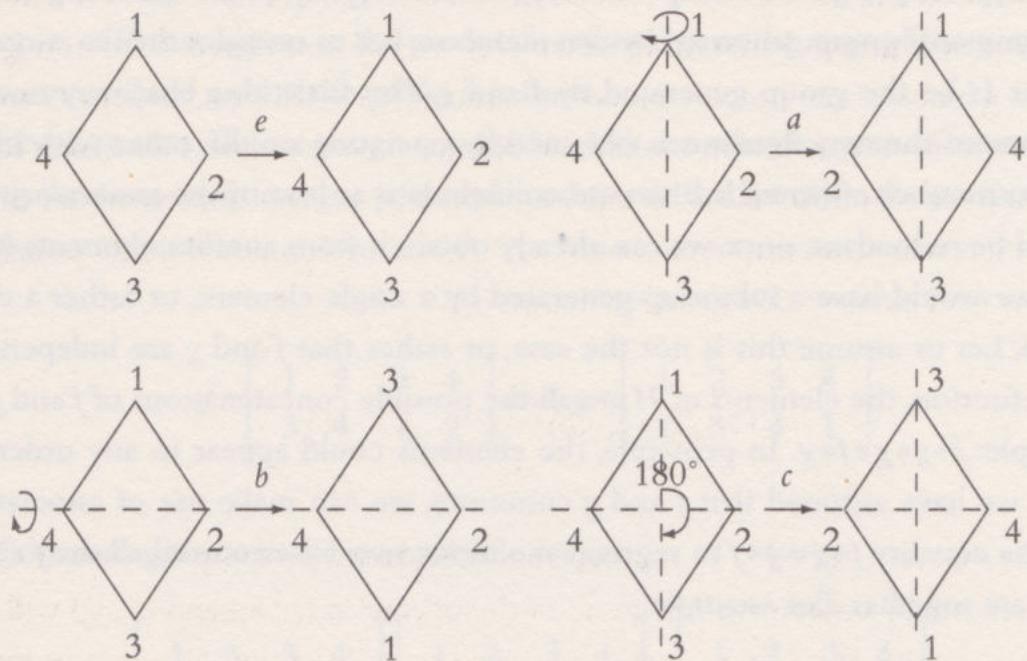
Transformation groups that leave the rhombus invariant.

All the elements of the Klein group have order two; this is why the only element to appear in the diagonal of the multiplication table is the identity element. In fact, it is possible to show that the only groups of order four are the cyclic group $\mathbb{Z}/4$ and the Klein group and the criteria for distinguishing them is precisely the existence of elements of order four.

LÉVI-STRAUSS: I understand, Mr Weil, but I have the feeling that we are getting off track. What does this have to do with marriages?

WEIL: You are so impatient! Before, I told you that in a society that conforms to our hypothesis, knowledge of the structure of kinship is reduced to the types of marriage M_i and the functions f and g. Let us now introduce a third hypothesis, related to the limits of the prohibition of incest and which appears to hold for some of the tribes you study in *The Elementary Structures of Kinship*:

> **Hypothesis 3**: The marriage between any man and the daughter of the brother of his mother is permitted.

As I have explained to you, this condition equates to the commutativity of f and g. Therefore, in order to study all the possible models of societies that satisfy the three hypotheses, we would, in some way, need to classify the abelian subgroups of the symmetry group generated by two elements. Let us consider them:

Let H be the group generated by f and g. The first thing that may occur is that one of the two elements is obtained by operating on the other with itself a certain number of times. In this case, to include it as part of the generators of H would be redundant, since we can already obtain it from another element, and in fact, we would have a subgroup generated by a single element, or rather a cyclic group. Let us assume this is not the case, or rather that f and g are independent. By definition, the elements of H are all the possible concatenations of f and g, for example: $f*g*g*f*g$. In principle, the elements could appear in any order, but since we have assumed that f and g commute, we can make use of associativity and the equality $f*g=g*f$ to regroup the terms two-by-two until all the f and all the g are together. For example:

$$f*g*g*f*g = f*g*(g*f)*g = f*g*(f*g)*g = f*(g*f)*g*g = f*(f*g)*g*g = f^2*g^3.$$

As this procedure is valid for any element of H, we have shown that all the elements can be written in the form f^n*g^m, where n and m are natural numbers (they may be zero). The standard convention is that both f^0 and g^0 are the identity element, such that when an index is cancelled, we recover the powers of the other term. The idea is that, instead of f^n*g^m, we could have written (f^n, g^m) without making a substantial change to the structure of H. This looks highly similar to the product of two cyclic groups, although the terms f^n*g^m can be repeated, even if we

choose n and m to be less than the orders of f and g respectively. Some work is still required to show that H is a product of two cyclic groups[1]:

Proposition 1: A finite abelian group generated by two elements is cyclic or the direct product of two cyclic groups.

In fact, the result is a specific case of the *fundamental theorem of finitely generated abelian groups*, which states that any finitely generated abelian group is isomorphic to a direct product of the form

$$\mathbb{Z} \times .... \times \mathbb{Z} \times \mathbb{Z}/n_1 \times ... \times \mathbb{Z}/n_k,$$

where $\mathbb{Z}$ is the group of integers and $\mathbb{Z}/n_1, ..., \mathbb{Z}/n_k$ are cyclic groups. The number of copies of $\mathbb{Z}$ that appear in the product is referred to as the *range* of the group and is non-zero if and only if the group is infinite.

LÉVI-STRAUSS: Before we go any further, let's see what happens in an example. Using the same notation that you explained to me the last time, the permutations f and g are written as

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} \text{ and } g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}.$$

Composing them in the two possible orders

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

we can see that they commute. Therefore in our generalised exchange structure any man can marry the daughter of the brother of their mother.

---

1 The interested reader will find a full proof in the Appendix. To understand it correctly, it will be helpful to have read the first part of the following chapter.

WEIL: Since the subgroup of S_4 generated by f and g is abelian, it must be a cyclic group or the direct product of two cyclic groups. In this case, the calculation

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix}$$

shows that the permutation f is obtained by composing g with itself ($f=g^2$), hence we are faced with the first of the two possible situations. Is this always the case? The answer is no. Let me exhibit an example in which the subgroup generated by f and g is the direct product of the two cyclic groups. Imagine that the types of possible marriages are:

(M_1) man A with woman D

(M_2) man B with woman C

(M_3) man C with woman B

(M_4) man D with woman A

$A \rightleftarrows D$

$B \rightleftarrows C$
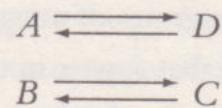
In this case the clans A and D swap women and the same happens with B and C, hence we find ourselves dealing with a 'restricted exchange'. Furthermore, imagine that the children of mothers from clans A, B, C and D are of clans B, A, D and C respectively. We can calculate the functions f and g as above:

Parents	M_1	M_2	M_3	M_4
Son $f(M_i)$	M_3	M_4	M_1	M_2
Daughter $g(M_i)$	M_2	M_1	M_4	M_3

Note that f is the same permutation from the previous example, but that g has changed. Even so, both continue to commute, since:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}.$$

The difference with respect to the previous situation is that now both f and g are elements of order two (you do the maths!) Therefore none of them can be the result of repeatedly applying the other. The subgroup generated by f and g will be the product of two cyclic groups In fact, this is the Klein group!

LÉVI-STRAUSS: Another of the reasons why ethnologists are interested in studying the marriages of a tribe consists of determining whether it is possible to find sub-populations that do not maintain ties of kinship with each other. In this case, the society is said to be *reducible*. Let me show you an example. Imagine that an elementary tribe made up of four clans has restricted exchange:

(M_1) man A with woman B

(M_2) man B with woman A

(M_3) man C with woman D

(M_4) man D with woman C

$$A \rightleftarrows B$$
$$C \rightleftarrows D$$
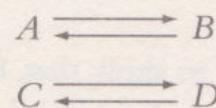
and that the children belong to the same clan as their mother. The calculation of the functions f and g is carried out in the same way as always, but there is no harm in refreshing our memory. In a marriage M_1, the woman is from clan B, and so are her children. A man B marries according to the rule M_2, hence $f(M_1) = M_2$, while $g(M_1) = M_1$, since the women B must follow the first rule. Following the same strategy for the other marriages gives the table

Parents	M_1	M_2	M_3	M_4
Son $f(M_i)$	M_2	M_1	M_4	M_3
Daughter $g(M_i)$	M_1	M_2	M_3	M_4

which clearly shows that the clans A and B never mix with C and D. Hence, the society is *reducible*. Otherwise, we say that it is *irreducible*.

WEIL: Note, Mr Lévi-Strauss, it suffices to consider irreducible societies since each tribe can be broken down into irreducible sub-populations. This is just an example of a general principle that is applied in many branches of mathematics. If an object is made up of simple objects and we can control the decomposition, then it is sufficient to study the latter to understand the whole. Let's translate irreducibility into the language of group theory. A society is irreducible if and only if any two types of marriage are connected by the permutations f and g, in other words if it

is possible to obtain one from the other by applying these operations. Don't forget that f and g allow us to construct the entire family tree! It is clear that this property does not hold for the tribe in your example, since applying f and g to M_1 only gives the marriages M_1 and M_2. However, our first two societies were irreducible. Recall the table that we began with:

Parents	M_1	M_2	M_3	M_4
Son $f(M_i)$	M_3	M_4	M_1	M_2
Daughter $g(M_i)$	M_2	M_3	M_4	M_1

I am going to show that, based on marriage M_1, it is possible to obtain all the others. Indeed, applying f and g gives M_3 and M_2, respectively. No mystery here! On the other hand, if I first apply f and then g, I obtain M_4, as a result of the equalities $g(f(M_1)) = g(M_3) = M_4$. All we need to do now is see how to obtain M_1; one possibility is to apply f twice, since $f^2(M_1) = f(M_3) = M_1$. Now we have them all! Hence, the society is irreducible.

LÉVI-STRAUSS: Hold on a minute, do you not have to show that the same is true if, instead of M_1, we start with M_2, M_3 and M_4?

WEIL: That is not necessary; let me explain why. We know that, starting from M_1 it is possible to obtain all the types of marriage. Imagine we wish to do the same with any of the other M_i. Let h be the element of the subgroup generated by f and g that makes it possible to go from M_1 to M_i, or in other words, the condition $h(M_1) = M_i$ holds. Since we are dealing with a group, h has an inverse h^{-1} that works in the opposite direction. Applying h^{-1} to both sides of the equality gives $h^{-1}(h(M_1)) = h^{-1}(M_i)$. However, h^{-1} composed with h gives the identity; remember the definition of the inverse element! Hence, $M_1 = h^{-1}(M_i)$. This means that starting from M_i, we can reach M_1. Since M_1 was connected to the other types of marriage, it will also be connected to any of the M_i. The subgroups of S_n that satisfy this property are referred to as *transitive*. Therefore:

> A tribe made up of n clans is irreducible if and only if the subgroup S_n generated by the permutations f and g is transitive.

Combining this result with proposition 1, it is clear that, to study the irreducible societies that conform to our three hypotheses, we must know a) which cyclic subgroups of S_n are transitive, and b) which direct products of two cyclic subgroups of S_n are transitive. An extremely simple general observation is that a subgroup H of S_n can only be transitive if it has at least n elements. Imagine if it had less, so that $m < n$, and let $h_1, h_2 \ldots h_m$ be the elements of H. This means the marriages connected to M_1 will be $h_1(M_1), h_2(M_2) \ldots h_m(M_1)$. In the best case, they will all be different, but they will never cover them all, since there are m, and m is less than n. Making use of some additional properties of the symmetric group, it is not hard to see which are the transitive cyclic subgroups of S_n, but let us leave this, otherwise we'll never finish with the marriages.

The Murngin

LÉVI-STRAUSS: Although your conceptual explanation is much more satisfactory than the ones proposed by the first anthropologists, in all the examples we have considered until now, it has been possible to solve the problem by explicitly enumerating all the possible combinations. The point at which group theory really does become essential is the point at which the number of clans grows or the marriage rules alternate exogamic and endogamic elements. I realised this as soon as I began to study the Murngin tribe, a group of aboriginals that live in the northern tip of Australia, in Arnhem Land. Shortly before I was to begin my PhD thesis, one of the leading experts on Australian aboriginals, Professor Elkin, had written that there was no point in conducting a purely formal analysis of the systems of aboriginal kinship since this would not contribute any real knowledge of the customs of the tribe. However, fully understanding the structure of the Murngins was crucial, since it is one of the few restricted exchange systems that distinguish *cross-cousins* – marriage with the daughter of the brother of the mother is permitted but it is prohibited with the daughter of the sister of the father. Since none of the systems known at that point made it possible to explain this dichotomy, some authors had chosen the simplest solution – they regard it as a system without a pattern. However, how could it be possible that a rule as precise as the dichotomy between cross-cousins, which is the logical consequence of a specific initial configuration, appears in a system not governed by any law.

The Murngin are divided into two sections, the Yiritcha and the Dua, each of which is made up of four clans called Ngarit, Bulain, Kaijark, Bangardi, Buralang,

Balang, Karmarung and Warmut. The names are not important. We will represent them using the symbols A_1, A_2, B_1, B_2, C_1, C_2, D_1 and D_2. So far, everything seems normal, but soon an anomaly that characterises all the systems of this region appears: the men are not always required to choose their wives from the opposite section. In fact, there are two alternatives: (I) and (II), the former within the same section and the latter in the other. They are represented in this diagram:

$$A_1 \rightleftarrows B_1$$
$$A_2 \rightleftarrows B_2$$
$$C_1 \rightleftarrows D_1$$
$$C_2 \rightleftarrows D_2$$

(I)

$$A_1 \quad B_1$$
$$A_2 \quad B_2$$
$$C_1 \quad D_1$$
$$C_2 \quad D_2$$
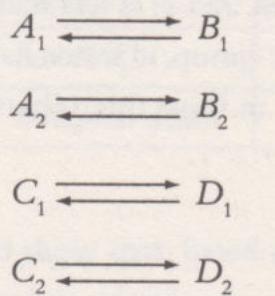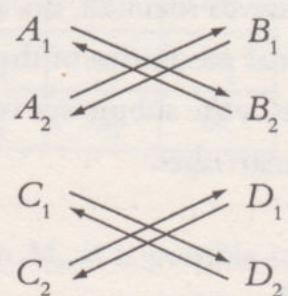
(II)

What cannot change in the Murngin is the way in which the mother determines the clan of her children. In this case, the following rule applies:

Mother	A_1	A_2	B_1	B_2	C_1	C_2	D_1	D_2
Sons	C_2	C_1	D_2	D_1	A_1	A_2	B_1	B_2

WEIL: For the society to satisfy our hypotheses, it is necessary to assume that the fact that an individual is governed by formula (I) or formula (II) only depends on their sex and the type of marriage, (I) or (II), of their parents. For each clan, there are two types of marriage, giving 16 different rules. Instead of enumerating each of them M_1, M_2... M_{16}, I am going to describe a smarter system of notation that will facilitate the calculations. First of all, let us assign each of the clans of the tribe a triple (a, b, c) composed of zeros and ones, where

a is 0 if the clan is A or B, and 1 if the clan is C or D

b is 0 if the clan is A or C, and 1 if the clan is B or D

c is 0 if the number of the subclass is 1, and 1 if it is 2.

For example, an individual of clan A_1 will be represented by the triple $(0, 0, 0)$, whereas another from clan B_2 will be represented by $(0, 1, 1)$. Conversely, if we are

78

given a triple of zeros and ones, such as $(1, 0, 0)$, it is possible to uniquely identify the clan to which they belong. In this case, since the first coordinate is 1, the clan will be C or D. Since the second coordinate is 0, we also know that the clan is A or C. Therefore, the only possibility compatible with the two conditions is that the individual belongs to clan C. Since the last coordinate is 0, they belong to clan C_1.

LÉVI-STRAUSS: Now we need to represent the marriages...

WEIL: Exactly! If we have assigned a triple to each clan (a, b, c), we can add a fourth coordinate to specify the formula for the marriage. Hence, each of the M_i will be substituted for four numbers (a, b, c, d), that can be either zero or one. The first three (a, b, c) indicate the clan of the man getting married, and the fourth is 0 or 1 depending on whether the marriage is carried out according to formula (I) or (II). For example, in the marriage $(1, 0, 0, 1)$ a man from class $(1, 0, 0)$, or rather, C_1, marries according to formula (II). Therefore he marries a woman of type D_2, or in other words $(1, 1, 1)$. This also determines the type of the children, who in this case will be of clan B_2, or $(0, 1, 1)$. To summarise:

Type of marriage	$(1, 0, 0, 1)$
Clan of father	$(1, 0, 0)$
Clan of mother	$(1, 1, 1)$
Clan of children	$(0, 1, 1)$.

The most important reason for introducing this notation using zeros and ones is that it allows us to represent kinship relations through addition in the cyclic group $\mathbb{Z}/2$. To be fully rigorous, we would need to write each of the zeros and ones in square brackets, but it's best not to complicate the notation. Thanks to this formulation, the situation for the example above can be generalised using two lemmas I will state now:

Lemma 1: In a marriage of type (a, b, c, d), the woman belongs to the clan $(a, b+1, c+d)$.

In fact, men who marry according to the rule (a, b, c, d) are from clan (a, b, c). The first observation is that, regardless of the formula for the marriage, the individuals of the clans A and B marry among each other, and the same happens with C and D.

Since a is 0 if the clan is A or B, and 1 if it is C or D, the first coordinate associated with the woman will coincide with that of the man. Let's see what happens to the second. To do so, we must remember that, regardless of the formula of the marriage, the men from clans A and C marry women from clans B and D, respectively. Hence, if $b=0$, the second coordinate for the woman will be 1. Similarly, the men from clans B and D marry women from A and C; hence if $b=1$, the second coordinate for the woman will be 0. In both cases b becomes $b+1$, since $0+1=1$ and $1+1=0$ in $\mathbb{Z}/2$. All we need to do now is study how the third coordinate changes, which represents the subclass. This is the only part that depends on the formulae (I) and (II). If we are dealing with the first case, or rather if $d=0$, all the men marry women of the same subclass, hence the third coordinate does not change. However, according to formula (II), or rather when $d=1$, the subclasses are switched. But this is nothing more than adding d to the last coordinate. Lemma proved! A similar argument allows us to determine the class to which the children belong depending on the mother. Let's see:

> **Lemma 2:** The children of a woman of class (x, y, z) belong to the clan $(x+1, y, x+z+1)$.

Now that we know how the clan of the woman determines each of the marriages and how she transfers this to her children, we can combine both results to describe the clan of the descendants depending on the type of marriage of the parents. Imagine that we begin with a marriage (a, b, c, d). By the first lemma, the women will be of class $(a, b+1, c+d)$. If we now substitute in the statement of the second lemma $x=a, y=b+1, z=c+d$, we reach the conclusion that the children will be of class $(a+1, b+1, a+c+d+1)$. To summarise:

> **Lemma 3:** The children of a marriage of type (a, b, c, d) belong to the clan $(a+1, b+1, a+c+d+1)$.

LÉVI-STRAUSS: The only information we are missing to determine the functions f and g is how the children inherit the preference for model (I) or (II). The fieldwork indicates that only the following four situations can arise:

(1) The children retain the formula of their parents.

(2) The children invert the formula of their parents.

(3) The sons retain the formula and the daughters invert it.

(4) The sons invert the formula and the daughters preserve it.

WEIL: We can symbolise each of these two cases using two indices (p, q), where p is 0 if the sons preserve the marriage formula of their parents, and 1 if they do not, and likewise with q for the daughters. In this way, the four possibilities that you have mentioned become $(0, 0)$, $(1, 1)$, $(0, 1)$ and $(1, 0)$. Note, Mr Lévi–Strauss, that if a marriage is determined by the formula associated with the coordinate d, the sons will follow the rule $d + p$, and the daughters, $d + q$. This information allows us to write the function f. Starting with a marriage (a, b, c, d), we know by lemma 3 that the children belong to clan $(a + 1, b + 1, a + c + d + 1)$ and, by the reasoning above, the formula for their marriage is $d + p$. Therefore:

$$f(a, b, c, d) = (a + 1, b + 1, a + c + d + 1, d + p).$$

To calculate g, another step is required. Although we know that the daughters of a marriage (a, b, c, d) are of class $(a + 1, b + 1, a + c + d + 1)$, the first three coordinates of the marriage we must assign them do not represent their clan, but the clan of the man they will marry. Hence, we must consider the class of the men that marry the women of class $(a + 1, b + 1, a + c + d + 1)$ according to the formula $d + q$. In fact, we need a result complementary to lemma 1. Let us recall what it says, changing the letters to avoid confusion:

Lemma 1: In a marriage of type (x, y, z, t), the women belongs to class $(x, y + 1, z + t)$.

We know that $t = d + q$ and that $(x, y + 1, z + t) = (a + 1, b + 1, a + c + d + 1)$, since this is the clan to which the woman belongs. Equating the coordinates gives the following system of equations:

$$x = a + 1, \qquad y + 1 = b + 1, \qquad z + d + q = a + c + d + 1,$$

in which I have substituted t for its value $d+q$. For the first, there is nothing to be done, since we already know the value of x. I hope you have not forgotten the property of elimination I explained to you last time, Mr Lévi-Strauss. If we apply it to the last two equations, we have

$$y = b, \qquad z + q = a + c + 1.$$

This gives the value of y. To calculate the value of z, note that in the cyclic group $\mathbb{Z}/2$, the result of adding an element to itself is always zero, since $0 + 0 = 1 + 1 = 0$. Hence, if I add q to both sides of the equality, I will have $z = a + c + q + 1$. To summarise, if a woman of class $(a+1, b+1, a+c+d+1)$ marries according to the formula $d+q$, their complete type of marriage is

$$g(a, b, c, d) = (a+1, b, a+c+q+1, d+q).$$

LÉVI-STRAUSS: Now I remember why I asked for your help, Mr Weil…

WEIL: I must admit, Mr Lévi-Strauss, that I also struggled to find the right formalism… What is important is that once we have calculated the functions f and g, answering your question about how the formulae (I) and (II) are transmitted to the children so that, in the following generation, a man is still allowed to marry the daughter of the brother of his mother automatically. Indeed, this property is equivalent to the commutativity of the permutations f and g. Let's carry out the calculation. On the one hand:

$$g(f(a, b, c, d)) = g(a+1, b+1, a+c+d+1, d+p)$$
$$= ((a+1)+1, b+1, (a+1)+(a+c+d+1)+q+1, (d+p)+q)$$
$$= (a, b+1, c+d+q+1, d+p+q),$$

since we can simplify the elements that are added twice in each of the coordinates. On the other hand:

$$f(g(a, b, c, d)) = f(a+1, b, a+c+q+1, d+q)$$
$$= ((a+1)+1, b+1, (a+1)+(a+c+q+1)+(d+q)+1, (d+q)+p)$$
$$= (a, b+1, c+d+1, d+p+q),$$

after carrying out the same simplifications. Therefore, the condition that must be verified is the following:

$$(a, b+1, c+d+q+1, d+p+q) = (a, b+1, c+d+1, d+p+q).$$

Since the first, second and fourth coordinates are the same, we need only concern ourselves with the third. Thanks to the property of elimination, the equality $c+d+q+1=c+d+1$ is equivalent to $q=0$. Remember that this means the formula for the marriage of the daughters must be the same as the one for the parents. Therefore the property we are looking for only holds in societies in which the formula for marriage is transmitted according to models (1) or (4). In other words, either the children of both sexes preserve it or it is inverted by the sons, in which case the women conserve it. Let's look at both cases.

The first of these societies is clearly reducible, since the formula (I) or (II) for the children always coincides with that of their parents, the type of marriage is maintained throughout the family tree. Therefore, the tribe can be broken down into two sub-populations: those who marry according to formula (I) and those who marry according to formula (II). As we can see from the table, the elements f and g both have order four, but their squares are the same:

f	$(a+1, b+1, a+c+d+1, d)$	$(a+1, b, a+c+1, d)$	g
f^2	$(a, b, c+1, d)$	$(a, b, c+1, d)$	g^2
f^3	$(a+1, b+1, a+c+d, d)$	$(a+1, b, a+c, d)$	g^3
f^4	(a, b, c, d)	(a, b, c, d)	g^4

LÉVI-STRAUSS: This means that in this tribe a man can marry the daughter of the sister of his father.

WEIL: The equality $f^2=g^2$ also implies that the group generated by f and g does not have 16 elements, as we would expect, but only eight: $e, f, f^2, f^3, g, fg, f^2g$ and f^3g. Therefore, the society is reducible. In fact, this group is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/4$.

LÉVI-STRAUSS: Let us now study the remaining case. Here the sons invert the marriage formula of their parents, whereas the daughters preserve it, and hence $p=1$ and $q=0$. As such, the functions f and g are:

$$f(a, b, c, d) = (a+1, b+1, a+c+d+1, d+1), \qquad g(a, b, c, d) = (a+1, b, a+c+1, d);$$

g is the same as before; we already know it is of order four. Let's calculate the order of f. To do so, we must repeatedly apply it until reaching the identity. However, unless I'm wrong, in this case we need only do so twice, because

$$f^2(a, b, c, d) = f(a + 1, b + 1, a + c + d + 1, d + 1)$$
$$= ((a+1) + 1, (b+1) + 1, (a+1) + (a+c+d+1) + (d+1) + 1, (d+1) + 1)$$
$$= (a, b, c, d),$$

using the simplifications that you have taught me. Furthermore, we can see that f and g are independent, hence the subgroup they generate is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/4$. This is enough to show that this tribe is not irreducible either, since there are not enough elements in the group $\mathbb{Z}/2 \times \mathbb{Z}/4$, which has order eight, to transform the 16 types of marriage amongst each other.

WEIL: Splendid, Mr Lévi-Strauss! You have understood everything! In this case, it is also possible to show that the society is reducible using a more direct method. I shall explain it to you so that you can learn a new technique. Let's begin with a marriage of the type (a, b, c, d). According to our calculations, the sons marry according to $(a + 1, b + 1, a + c + d + 1, d + 1)$. The crucial observation is that, if I subtract the fourth coordinate from the second, I get:

$$(b + 1) - (d + 1) = b - d,$$

the same as we started with! Mathematicians say this quantity is *invariant* with respect to the operation f. It continues to be so, perhaps more clearly, when I apply g, since in this case the second and the fourth coordinates do not change. Hence, the successive composition of f and g only allows us to reach the marriages in which $b - d$ has the same initial value. For example, starting with $(1, 1, 1, 0)$ we can never obtain $(1, 0, 1, 0)$, because in the first instance, the difference between the second and fourth coordinates is 1, whereas in the second it is 0. This means that members of class D_2 who marry according to (I) belong to a different sub-population from those from class C_2 who obey the same formula. With a little more work, these two sub-populations can be explicitly determined:

Sex	Class	Formula
Man	A or C	(I)
Man	B or D	(II)
Woman	A or C	(II)
Woman	B or D	(I)

First sub-population.

Sex	Class	Formula
Man	*A* or *C*	(II)
Man	*B* or *D*	(I)
Woman	*A* or *C*	(I)
Woman	*B* or *D*	(II)

Second sub-population.

LÉVI-STRAUSS: It's enough to make you think that the Murngin are aware of group theory…

WEIL: When I think of a system which at first sight threatens to be of indecipherable complexity but is transformed into something as simple as an abelian group after introducing the correct notation, the word miracle comes to mind. I wouldn't dare to say that the tribe has adopted the principle that any man can marry the daughter of the brother of their mother just to please mathematicians – that would be going too far – but I must recognise that I still feel a special tenderness for the Murngin to this day. With examples such as this one, it is difficult not to remember the sonnet in which Michelangelo explains how a block of marble already contains the sculpture, such that the work of the artist is reduced to removing the unwanted stone:

> "Non ha l'ottimo artista alcun concetto
> c'un marmo solo in sé non circonscriva
> col suo superchio, e solo a quello arriva
> la man che ubbidisce all'intelletto".[2]

The mathematician is also a great sculptor of extremely hard and strong material. So subject is he to its imperfections that this gives the work a sort of objectivity.

---

2 Not even the best of artists has any conception / that a single marble block does not contain / within its excess, and that is only attained / by the hand that obeys the intellect.

Chapter 5

Under the Sign of Diophantus

Fourier believed that the main goals of mathematics were to serve the common good and to explain natural phenomena. However, a philosopher like him should have known that science is solely for the honour of the human spirit and that, in this respect, a question about numbers is as important as a question about the system of the world.

C.G.J. Jacobi, letter to Legendre

LÉVI-STRAUSS: Do you remember that in one of our conversations you promised that you would explain the problem from your PhD thesis in more detail?

WEIL: How could I forget! However, this time, if it's okay with you, let us change the method. I have written some detailed notes you can read and then you can ask me about what you don't understand. Are you ready?

*****

Almost everything about the mathematical life of Diophantus of Alexandria is a conjecture. The only thing we know for sure is the age at which he died, thanks to an epigram in the form of a riddle in the *Palatine Anthology*. It goes like this: "This tomb holds Diophantus. Ah, what a marvel! And the tomb tells scientifically the measure of his life. God vouchsafed that he should be a boy for the sixth part of his life; when a twelfth was added, his cheeks acquired a beard. He kindled for him the light of marriage after a seventh, and in the fifth year after his marriage He granted him a son. Alas! late-begotten and miserable child, when he had reached the measure of half his father's life, the chill grave took him. After consoling his grief by this science of numbers for four years, he reached the end of his life." Indeed, if we let x be the number of years for which Diophantus lived, the epigram can be translated into the following first-degree equation

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4,$$

and after a few elementary operations, we can conclude that Diophantus lived for 84 years. This equation is much simpler than the ones that earned this Alexandrian sage a place in the history of mathematics. In the books that make up *Arithmetica*, Diophantus began the study of the integral roots of polynomial equations, now referred to as *Diophantine* equations in his honour. This class contains, for instance, equations of the form $x^n + y^n = z^n$. When the exponent is 2, there is an infinite number of positive solutions, but if n is greater than or equal to 3, there is none. The first person to realise was the Frenchman, Pierre de Fermat, when he was studying Diophantus' *Arithmetica*. On its pages, he wrote that he knew of a marvellous proof, but that there was not sufficient space in the margins to write it out in full. It took three and a half centuries to discover the first proof of what came to be known as 'Fermat's last theorem' and which involved techniques much more complex than the ones the French mathematician would have been able to use at the time. Despite their innocent appearance, the Diophantine equations represent one of mathematics' hardest problems. For this reason, here we shall limit ourselves to the simplest cases: linear equations, the Pell–Fermat equation and elliptic curves.

Background

We need some background in order to be able to tackle the study of Diophantine equations. As different types of numbers will appear throughout these notes, let me say something about them. On the one hand, we have the *natural* numbers, used for counting: 0, 1, 2, 3… Given two natural numbers, we can calculate their sum. However, this operation does not form a group because for an inverse element to exist, we would also need to consider negative numbers. Adding them gives the abelian group of the *integers*: 0, 1, –1, 2, –2, 3, –3… In fact, this structure is a little more rich, since it has two operations instead of one. As well as addition, we also have multiplication. However, the multiplication of two non-zero integers suffers from the same problem – it does not define a group structure, since, by means of example, for element 2 to have an inverse, we would also need to include the number 1/2. This problem is solved by considering all the fractions a/b, where a and b are two integers (b is non-zero) that make up the set of *rational* numbers. Each of these can be associated with a periodic decimal expression – for example, 1/3 is 0.3333… and

2/11 is 0.181818… However, if we only allow periodic expressions, equations as simple as $x^2 = 2$ do not have solutions, since the decimal expansion of the square root of 2 is not periodic; it is an *irrational* number. To obtain even more solutions, we can consider all decimal expressions, even when they do not have a pattern that repeats. This gives us the *real* numbers.

However, let us return to the *natural* numbers which, according to Kronecker, are the work of God. Given two natural numbers m and n, we say that *m divides n*, or that *n is divisible by m*, or *m is a divisor of n*, if the result of dividing n by m gives another natural number. For example, 2 divides 10 since 10 over 2 is 5, which is a natural number; but 2 does not divide 15, since 15 over 2 is 7.5; the result is not 'exact'. Hence, when n is divisible by m, there is another natural number k such that n is the product of m and k: $n = m \cdot k$. Note that the divisors of a number are always less than or equal to the number, and that any number is divisible by 1 and itself. Sometimes these are the only divisors, in which case we say that the number is *prime*. Hence, 5 is prime since neither 2, nor 3, nor 4 divide it, but 6 is not, since it is divisible by 2 and 3. The first prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23… and it can be shown that this list is endless.

The importance of the prime numbers lies in the fact that they are the fundamental building blocks of arithmetic – all numbers are obtained from prime numbers. Indeed, if n is not a prime number, there is a natural number that lies strictly between 1 and n that divides it. This allows the number to be broken down in the form $n = a \cdot b$. For example, if the original number was 30, we would have $30 = 2 \cdot 15$. Hence, we have obtained two numbers a and b to which we can apply the process once again. If both are prime, we are done; but if one is non-prime, we must rewrite it as the product of two factors. In this example, 2 is prime, but 15 can be written as 3 times 5, such that $30 = 2 \cdot 3 \cdot 5$. As all the factors are now prime, the game is over. In general, at each step we find a prime factor or a decomposition into two smaller numbers, which guarantees that sooner or later, the algorithm will come to a halt.

The Fundamental Theorem of Arithmetic. Any natural number can be written as a product of primes.

In spite of the simplicity of the argument we have used to show the fundamental theorem of arithmetic, the problem of writing a number in terms of its prime factors can be insoluble in practice. For example, if n is the product of two prime numbers

p and q, each of which has 400 digits, even the most powerful computers would take the age of the universe to factorise it. As we shall see further on, this is one of the principles behind the RSA *public key encryption system*, which ensures the security of all our computer transactions.

Let us now introduce a new concept: given two natural numbers m and n, we use the term *greatest common divisor* to refer to the largest natural number that divides both m and n. We shall abbreviate it as gcd(m,n). When we have the factorisations of m and n, it is easy to calculate the greatest common divisor: we take the prime numbers that appear in both lists, raised to the lowest power. Imagine we want to calculate the greatest common divisor of $50 = 2 \cdot 5^2$ and $120 = 2^3 \cdot 3 \cdot 5$. The shared primes are 2 and 5, which appear with exponents 1 and 2 in the first case, and 3 and 1, in the second. Hence, the greatest common divisor will be $2^1 \cdot 5^1 = 10$. However, we have already said that in practice factorising a number is an insoluble problem since the method fails when m and n are extremely large numbers.

Fortunately, we have another procedure for calculating the greatest common divisor, known as *Euclid's algorithm*. It consists of the following: assume that m is greater than n. As a first step, divide m by n. Two things may occur: if the remainder is zero, n divides into m, hence n is the greatest common divisor; otherwise, we repeat the process, substituting m for n, and n, for the remainder r of the previous division, because it can be proved that the greatest common divisor of m and n is the same as that of n and r[1]. Let's now continue with our example. The remainder of dividing 120 by 50 is 20, and therefore we apply the algorithm to 50 and 20. The remainder of dividing 50 by 20 is 10, and we repeat the procedure with 20 and 10. However, this time the division is exact, which shows that the greatest common divisor is 10. In fact, this algorithm provides us with more information: using the last division with a remainder that is non-zero, we can write $10 = 50 - 2 \cdot 20$. Taking a step backwards, we know that $20 = 120 - 2 \cdot 50$, so if we substitute the value of 20 in the first equality, we obtain a relationship with integer coefficients between 120, 50 and 10:

$$10 = 50 - 2 \cdot (120 - 2 \cdot 50) = 5 \cdot 50 - 2 \cdot 120.$$

---

1 Let's prove this! Let $d = $ gcd(m,n) and assume that the quotient of dividing m by n is t, with remainder r, hence: $m = nt + r$. Note straight off that d divides into r. Indeed, by definition there are integers p and q such that $m = dp$ and $n = dq$. Substituting, we have $r = m - nt = dp - dqt = d(p - qt)$, hence d divides into r. To conclude that gcd$(n,r) = d$, it is enough to show that there cannot be a common divisor greater than d. Once again, this is deduced using the formula $m = nt + r$, since, if it existed, it would also divide into m and would thus be a common divisor of m and n greater than d, which contradicts the fact that d is the greatest.

In general, thanks to Euclid's algorithm, it is not only possible to calculate the greatest common divisor easily, but we also have:

> **Proposition:** Let m and n be two natural numbers and let d be their greatest common divisor. There exist two integers u and v such that $d = mu + nv$.

A particularly interesting case occurs when m and n do not have common divisors. In this case, their greatest common divisor is 1 and we say that they are *coprime* or *relatively prime*. According to the proposition we have stated above, there are two integers u and v such that $mu + nv = 1$. This relationship is referred to as *Bézout's identity*.

Another fundamental property is the following: if a number a divides a product bc, and we know that a and b are coprime, a must divide c. If this were not the case, a prime factor of a would also appear in b, and the numbers would not be coprime. On the other hand, if d is the greatest common divisor of a and b, there are two integers p and q such that $a = dp$, $b = dq$. This is the case provided we have a common divisor, but the fact that d is the largest allows us to state that p and q are coprime, since if this was not the case, a and b would have a common divisor greater than d.

Linear equations

We can now solve the Diophantine equations of the form $ax + by = c$, where a, b and c are any three integers. Solving this equation means finding all the pairs of integers (x, y) for which the equation $ax + by = c$ holds. Let us see how to do this: let d be the greatest common divisor of a and b. By definition, d divides the numbers a and b, which means it also divides the expression $ax + by$. Furthermore, since the equation we are dealing with establishes that $ax + by = c$, the number d must also divide c. Hence, if d does not divide c, there are no solutions. This is the case, for example, with $50x + 120y = 7$. According to our calculations, the greatest common divisor of 50 and 120 is 10, which does not divide 7. Hereafter, we assume that d divides c.

Hence, we can write $a = dp$, $b = dq$ and $c = dr$, with p and q coprime. Let us study the first case, for which $c = 0$, in other words the *homogeneous* equation $ax + by = 0$. Dividing the first term by d, we can see that it suffices to solve the equation $px + qy = 0$, or rather, $px = -qy$. To do so, we argue as follows: because px is equal to

$-qy$, the number p divides into qy. However, p and q are relatively prime, meaning that the only possibility is that p divides into y, or in other words there is an integer λ such that $y = \lambda p$. Similarly, we can show that q divides into x, such that there will be another integer μ such that $x = \mu q$. Substituting the values of x and y into the equation gives $\mu pq = -\lambda pq$, or rather, $\mu = -\lambda$, since the product pq is non-zero. Hence, the solutions to the equation $ax + by = 0$ are the pair $(q, -p)$ and all its multiples $(\lambda q, -\lambda p)$.

Let us now assume that c is non-zero. Given two solutions (x_0, y_0) and (x_1, y_1) to the equation $ax + by = c$, we have:

$$a(x_0 - x_1) + b(y_0 - y_1) = (ax_0 + by_0) - (ax_1 + by_1) = c - c = 0,$$

from which we can deduce that $(x_0 - x_1, y_0 - y_1)$ is a solution to the homogeneous equation $ax + by = 0$. Since all the solutions to this equation are of the form $(\lambda q, -\lambda p)$, there will be an integer λ such that $x_0 - x_1 = \lambda q$ and $y_0 - y_1 = -\lambda p$, which is the same as: $x_1 = x_0 - \lambda q$ and $y_1 = y_0 + \lambda p$. Put another way: there are infinite solutions, but all of these are deduced based on a specific solution (x_0, y_0). In fact, recalling that p and q are the result of dividing a and b by the greatest common divisor, we have shown that all the solutions are:

$$\begin{cases} x = x_0 - \lambda \dfrac{b}{gcd(a,b)}, \\ y = y_0 + \lambda \dfrac{a}{gcd(a,b)} \end{cases}$$

where (x_0, y_0) is a specific solution, and λ is any integer. Hence, all that remains is to describe a method for finding (x_0, y_0). However, this is easy when we know that p and q are coprime, since thanks to Bézout's identity, there are two integers u and v such that $pu + qv = 1$. Multiplying u and v by r gives two numbers $x_0 = ur$ and $y_0 = vr$ such that $ax_0 + by_0 = c$.

Let us consider an example. Imagine we want to solve the Diophantine equation $50x + 120y = 20$. We have already noted that the greatest common divisor of 50 and 120 is 10. Since 10 divides into 20, there is a solution to the equation. In this case, the simplified form is none other than $5x + 12y = 2$. Let's calculate the numbers we have called u and v. Since $1 = 5 - 2 \cdot 2$ y $2 = 12 - 2 \cdot 5$, we have

$$1 = 5 - 2 \cdot (12 - 2 \cdot 5) = 5 \cdot 5 - 2 \cdot 12,$$

in other words: $u = 5$ y $v = -2$. Multiplying by 2 gives us the specific solution $(10, -4)$, which can be used to calculate all the others:

$$\begin{cases} x = 10 - 12\lambda \\ y = -4 + 5\lambda \end{cases}$$

A brief digression on cryptography

Let's consider how Diophantine linear equations are used in the public key encryption system. Recall that, given a natural number n, the group of integers modulo n is made up of the elements $[0], [1], [2]\ldots [n-1]$, and that the 'clock addition' is carried out as follows: first we add the numbers together as if they were two normal numbers, then we subtract n from the result the number of times required to obtain a number between 0 and $n-1$. In fact, we can do the same with multiplication. For example, if $n = 7$, to calculate the product $4 \cdot 5$, we begin by doing the same as we would for two integers. This gives 20, although it is still necessary to subtract 7 as many times as required: doing so once gives 13, doing so again gives 6, which is less than 7. Hence, we have established that the product of 4 and 5 is 6 modulo 7. Let's now turn to cryptography.

Imagine that Bob wants to send a secret message to Alice. As it is possible to encrypt any type of information numerically, it is enough to solve the problem of how to send a number m securely. Bob knows Alice's *public key*, which is available to everybody, and Alice has a *private key*, which only she knows. We must consider three phases – generating the keys, encrypting the message and decoding it.

First we'll consider how the keys are generated. We choose two prime numbers p and q. In principle, it suffices that the product of p and q, which we shall call n, is greater than the number m we wish to transmit. However, the method will only be secure when p and q are sufficiently large such that no computer is able to factorise n in a reasonable period of time. Hence, we choose p and q, two coprime numbers, with between 300 and 400 digits each. Now we introduce the quantity $r = (p-1)(q-1)$ and choose a number e less than r and coprime with it. The pair (n, e) is the public key. To calculate the private key, it is necessary to solve the Diophantine equation $ex + ry = 1$. If we let d be the first coordinate of a solution, the private key is the pair (n, d).

Once both keys have been determined, the encryption system functions as follows: Bob encrypts a message by raising the number m to the power e, reduces the result modulo n and sends this number $c = m^e$ (modulo n) to Alice. To decode the message, Alice raises c to the power d established by the private key and reduces it modulo n. This simple operation is sufficient to recover the information, since it can be shown that c^d modulo n is always equal to m.

The Pell–Fermat equation

Having fully solved the case of Diophantine linear equations, now let's consider second-degree equations. We will focus on the equation $x^2 - dy^2 = 1$, where d is a positive integer.

This is a problem with a long history, referred to in the literature as the Pell–Fermat equation, despite the fact that John Pell never worked on it. It was Euler who erroneously attributed a method actually discovered by the English mathematician William Brouncker in response to a challenge by Fermat. First imagine that d is equal to 1, or in other words attempt to calculate the integer solutions to the equation $x^2 - y^2 = 1$. Since the subtraction of squares can always be written as a product using the formula

$$x^2 - y^2 = (x+y)(x-y),$$

it is necessary to solve the equation $(x+y)(x-y) = 1$. The only way for the product of two integers to be 1 is for both factors to be equal to 1 or −1. We'll consider both cases separately. In the first, we have:

$$\begin{cases} x+y = 1 \\ x-y = 1 \end{cases},$$

and, adding the two equations, we see that $2x = 2$, hence $x = 1$ and $y = 0$. Similarly, the solutions to the system $x+y = x-y = -1$ are $x = -1$ and $y = 0$. Therefore, the equation $x^2 - y^2 = 1$ has just two integer solutions: $(-1, 0)$ and $(1, 0)$. The same study allows us to exclude the case in which d is a *perfect square*, that is $d = e^2$, since in this case $x^2 - dy^2 = x^2 - e^2y^2 = x^2 - (ey)^2$, and the change of variable $z = ey$ returns us to the same equation $x^2 - z^2 = 1$, whose solutions we already know. From now on, let's assume that d is an integer that is greater than or equal to 2 and is not a perfect square.

An essential part of the analysis of first-degree equations consists of seeing how, using two solutions to $ax + by = c$, it is possible to obtain a pair of integers (x, y) such that $ax + by = 0$. In this case, we can see that if we have two solutions to the Pell–Fermat equation, it is possible to find a third. The basic idea is to factorise the expression $x^2 - dy^2$ as

$$x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d}).$$

These factors are no longer integers (they contain the square root of a number that is not a perfect square), therefore both numbers cannot be equal to 1 or -1. However, if (x_1, y_1) and (x_2, y_2) are solutions to the equation, then:

$$\begin{cases} (x_1 + y_1\sqrt{d})(x_1 - y_1\sqrt{d}) = 1 \\ (x_2 + y_2\sqrt{d})(x_2 - y_2\sqrt{d}) = 1 \end{cases}.$$

Multiplying the two equations gives:

$$(x_1 + y_1\sqrt{d})(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d})(x_2 - y_2\sqrt{d}) = 1. \quad (*)$$

Let us begin to regroup the terms with the positive sign in the middle:

$$(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = x_1x_2 + x_1y_2\sqrt{d} + x_2y_1\sqrt{d} + y_1y_2(\sqrt{d})^2.$$

The first crucial observation is that the product of the two factors has the same structure, since $(\sqrt{d})^2$ is the same as d by definition. In fact, if we introduce the notation $x_3 = x_1x_2 + dy_1y_2$ and $y_3 = x_1y_2 + x_2y_1$, we have the equality:

$$(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = x_3 + y_3\sqrt{d}.$$

Since we also know that

$$(x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = x_1x_2 - x_1y_2\sqrt{d} - x_2y_1\sqrt{d} + y_1y_2(\sqrt{d})^2 = x_3 - y_3\sqrt{d},$$

we can rewrite the equation ($\star$) in the form:

$$(x_3 + y_3\sqrt{d})(x_3 - y_3\sqrt{d}) = 1.$$

This equality shows that (x_3, y_3) is once again a solution to the Pell–Fermat equation. Hence, based on two solutions, we have obtained a third. Furthermore, since the formulae that define x_3 and y_3 only contain summations and products, if the solutions (x_1, y_1) and (x_2, y_2) were integers, this will also be the case for the solution we have just found.

Let us use $\bullet$ to designate the operation which, given two solutions, associates a third. Our goal is to show the following result:

Proposition: The operation $(x_1, y_1) \bullet (x_2, y_2) = (x_3, y_3)$ defmes an abelian group structure on the set of integer solutions to the Pell-Fermat equation.

The fact that the operation is commutative is clear from the definition since the values of x_3 and y_3 do not change if we switch the order of (x_1, y_1) and (x_2, y_2). Hence, it suffices to show that the three axioms for the definition of the group hold. The first of these − associativity − is, in this case, a simple consequence of the associativity of the product of real numbers. For the identity element, note that $(1, 0)$ is always a solution to $x^2 - dy^2 = 1$. Let's see what happens when we compose it with an arbitrary solution (x_2, y_2). According to our formulae, $x_3 = 1 \cdot x_2 + d \cdot 0 \cdot y_2 = x_2$ and $y_3 = 1 \cdot y_2 + x_2 \cdot 0 = y_2$, hence $(1,0) \bullet (x_2, y_2) = (x_2, y_2)$ and we have found the identity element. All that remains is to show that each solution has an inverse, or in other words, given (x_1, y_1), we can find another solution (x_2, y_2) such that $(x_1, y_1) \bullet (x_2, y_2) = (1, 0)$. The easiest case is to try with $(x_1, -y_1)$, which is also a solution, since the squares of a number and its opposite coincide. Indeed:

$$(x_1, y_1) \bullet (x_1, -y_1) = (x_1^2 - dy_1^2, -x_1 y_1 + x_1 y_1) = (1, 0),$$

since the pair (x_1, y_1) is a solution to $x^2 - dy^2 = 1$. This concludes the proof that the integer solutions to the Pell–Fermat equation form an abelian group. The question that naturally arises is, what kind of group?

Among all the positive solutions to the Pell–Fermat equation, let's use the term *fundamental solution* to denote the pair (x, y) that minimises the value

of $x^2 + y^2$. For example, if $d = 2$, the fundamental solution is $(3, 2)$. On the one hand, $3^2 - 2 \cdot 2^2 = 9 - 2 \cdot 4 = 1$, so this is a solution. We now need to show that it is the 'smallest', and to do so we see that none of the coordinates of a positive solution can be 1, since if $x = 1$, $y = 0$, which is not positive, and if $y = 1$, $x^2 = 3$, which does not have integer solutions. Hence, the only way of obtaining a solution that is smaller than $(3, 2)$ would be to consider the pair $(2, 2)$. However $2^2 - 2 \cdot 2^2 = -4$, and so this is not a solution. This shows that $(3, 2)$ is the fundamental solution. Composing it successively with itself according to the group law, we obtain infinite solutions to the Pell–Fermat equation. For example, $(3, 2)$ • $(3, 2) = (17, 12)$ and $(3, 2)$ • $(3, 2)$ • $(3, 2) = (99, 70)$ are new solutions to the equation; in fact there is an infinite number of them. However, it is not so easy to see that this gives us all the positive solutions:

> **Dirichlet's unit theorem:** All the positive integer solutions to the Pell–Fermat equation are obtained from the fundamental solution.

This theorem leads us to consider the cyclic group generated by the fundamental solution, which is isomorphic to the group of integer numbers. It contains all the solutions (x, y) where both coordinates are positive, but also the identity element $(1, 0)$ and all the inverses $(x, -y)$. Let's assume that (x, y) is one of these. Since $(-x)^2 = x^2$, the pair $(-x, y)$ is also a solution to the Pell–Fermat equation. However, now $-x$ is positive, hence this solution is one of those we already have in the cyclic group generated by the fundamental solution. It now suffices to add a sign, which mathematically corresponds to the direct product of the integers modulo 2.

To summarise: The set of integer solutions to the Pell–Fermat equation is a group isomorphic to $\mathbb{Z} \times \mathbb{Z}/2$.

Elliptic curves

We'll now move on to equations of degree three, and how to define a group structure on the set of solutions to the equation $y^2 = x^3 + ax + b$, where a and b are arbitrary rational numbers. In this case, our construction will be purely geometric. Let us begin by representing the pairs of real numbers (x, y) for which the condition $y^2 = x^3 + ax + b$ holds on the plane. Given values for one of the two variables, and solving the corresponding equation, we obtain a series of points that can be

joined using continuous lines. The result is a curve on the plane, referred to by mathematicians as *elliptic*. We'll consider an example: if $a = -2$ and $b = 1$, the equation is of the form $y^2 = x^3 - 2x + 1$. If we substitute x by 0, the term on the right has a value of 1, hence we must solve the equation $y^2 = 1$, which has two solutions: $y = 1$ and $y = -1$. This gives us two points on the curve: $(0,1)$ and $(0,-1)$. If, on the other hand, x was 1, we would have $y^2 = 0$ or, in other words, $y = 0$. Hence, we can add the point $(1,0)$ to the list. Continuing with $x = -1$, the term on the right will have the value $(-1)^3 - 2(-1) + 1 = -1 + 2 + 1 = 2$, which gives the equation $y^2 = 2$, the solutions of which are $y = \sqrt{2}$ and $y = -\sqrt{2}$. Hence, the points $(-1, \sqrt{2})$ and $(-1, -\sqrt{2})$ also lie on the curve. In this case, we are not dealing with integer solutions to the equation, but this is not important since in order to draw the curve, we must consider all the real solutions.
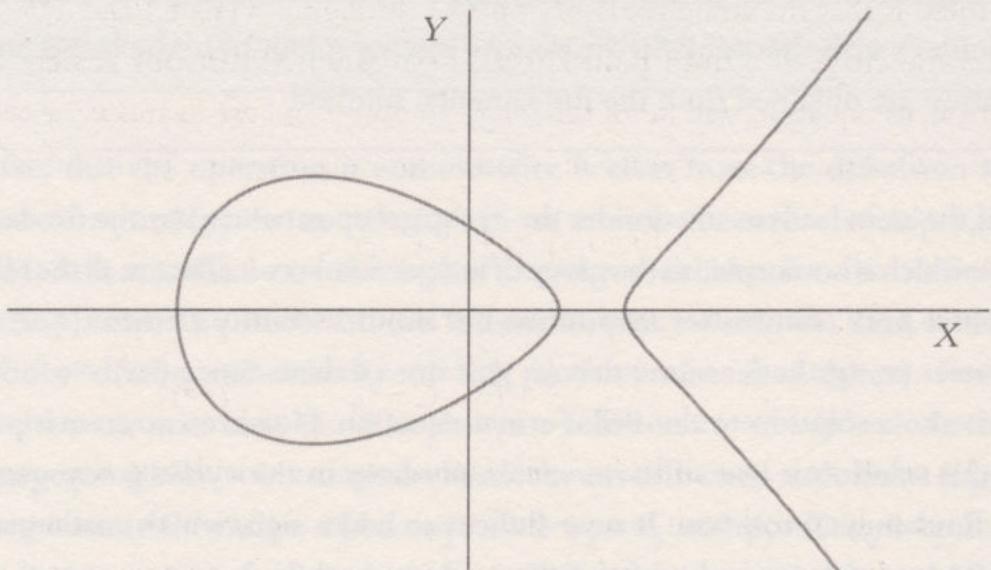
The elliptic curve $y^2 = x^3 - 2x + 1$.

Now that we have drawn the curve, let us take two different points on it, P and Q, and draw the straight line that joins them. We shall assume that P and Q are not symmetric with respect to the x axis, meaning that the line that passes through them will not be vertical. Let us note that this line cuts the curve at a third point, which we shall call PQ. Indeed, we can say that the result of operating on the points P and Q of the *elliptic curve* is the point that is symmetric to PQ with respect to the x axis, which we represent as $P + Q$:
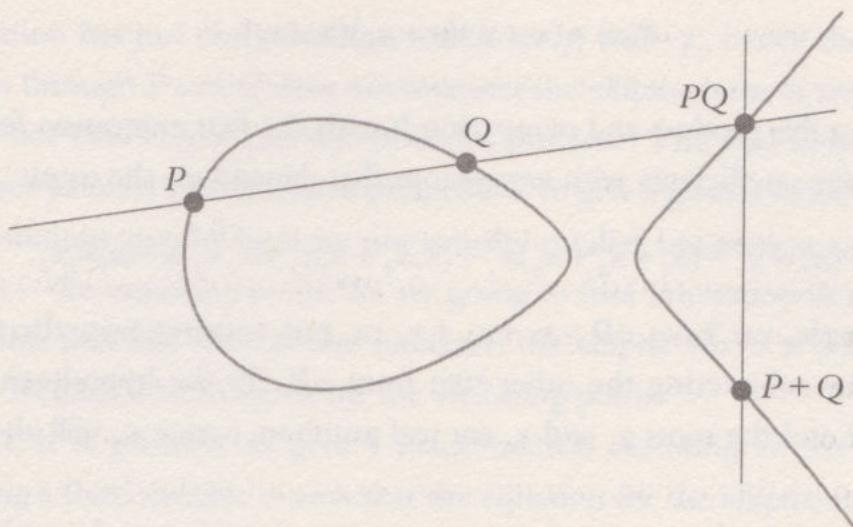
The sum of the points P and Q on the elliptic curve.

For this operation to be well defined, there is still a lot to be accounted for. The first of these is that the straight line that passes through $P=(x_1, y_1)$ and $Q=(x_2, y_2)$ intersects the curve at a third point. As we have assumed that this straight line is not vertical, its equation will be of the form $y = mx + n$, where m and n are two real numbers. Substituting this expression into the formula for our elliptic curve gives:

$$(mx+n)^2 = x^3 + ax + b,$$

which, after a few elementary operations, is transformed into:

$$x^3 - Ax^2 + Bx + C = 0, \qquad (\star\star)$$

where $A = m^2$, $B = a - 2mn$ and $C = b - n^2$. Hence, we are calculating the roots of a third-degree polynomial with real coefficients. We already know two of these: they are the x coordinates x_1 and x_2 of the points P and Q, since both belong to both the curve and the line. We can conclude thanks to the following result:

Lemma: If a third-degree polynomial with real coefficients has two real roots, the third root is also real.

Let us prove this. The simplest way to do so is as follows. Let

$$P(x) = x^3 + Rx^2 + Sx + T$$

be a third-degree polynomial with real coefficients. Let x_1, x_2, x_3 be its roots. Hence $P(x)$ can be written as

$$P(x) = (x - x_1)(x - x_2)(x - x_3).$$

Expanding this product and comparing it with the first expression for $P(x)$, we can identify the coefficients with expressions that depend on the roots:

$$P(x) = x^3 - (x_1 + x_2 + x_3)x^2 + (x_1 x_2 + x_1 x_3 + x_2 x_3)x - x_1 x_2 x_3.$$

For example, we have $-R = x_1 + x_2 + x_3$ or, put another way, the third root is obtained by subtracting the other two from $-R$. By the hypothesis, both the coefficient R and the roots x_1 and x_2 are real numbers, hence x_3 will also be a real number.

By virtue of the lemma we have just proven, there is a real number x_3 that satisfies the equation (∗∗). Substituting its value into the equality $y = mx + n$ gives us the coordinate y_3 of the point PQ. All that remains is to take the symmetric point, equivalent to considering the opposite y coordinate. Hence, the result of the operation for (x_1, y_1) and (x_2, y_2) will be the point $(x_3, -y_3)$.

Let us return to our example: as we have seen, the points $P = (0, 1)$ and $Q = (1, 0)$ lie on the elliptic curve of the equation $y^2 = x^3 - 2x + 1$. Let us calculate $P + Q$. To do so, we first need to determine the line that passes through P and Q. A simple calculation shows that its formula is none other than $y = -x + 1$. This gives the equation:

$$(-x + 1)^2 = x^3 - 2x + 1 \Leftrightarrow x^2 - 2x + 1 = x^3 - 2x + 1 \Leftrightarrow x^2 = x^3 \Leftrightarrow x^2(x - 1) = 0,$$

whose solutions are $x = 0$ (counted twice) and $x = 1$. Since $x_1 = 0$ and $x_2 = 1$, the point we are looking for is $x_3 = 0$. Substituting into the formula $y = -x + 1$, gives $y = 1$, such that the result of operating for P and Q is the point $P + Q = (0, -1)$. Note that, in this case, the result of operating on two integer solutions to the equation is also an integer solution. This is true in general, provided the coefficients of the equation are integers, and the proof is essentially the same, showing that, if a third-degree polynomial with real coefficients has two real roots, the third root is also real.

Hence, we have solved the first of our difficulties – showing that if a straight line passes through two non-symmetric points on the elliptic curve, it also intersects it at a third. However, what happens if the points P and Q are symmetric? In this case, we would have the coordinates $P = (x_1, y_1)$ and $Q = (x_1, -y_1)$, and the line joining them would be the vertical line given by $x = x_1$. However, when we come to substitute $x = x_1$ into the equation for the elliptic curve, we get $y^2 = x_1^3 + ax_1 + b$, in other words, the variable x has disappeared, and all that remains is y^2, which is a real number.

This equation has just two solutions, which are y_1 and $-y_1$, hence the straight line that passes through P and Q does not intersect the elliptic curve at any other point. PQ does not exist! How can we solve this problem? The idea dates back to the Renaissance painters who invented perspective. To give a greater sensation of realism in their paintings, parallel lines are not actually parallel, but cross at a point outside the canvas – the vanishing point. We are going to find inspiration in these painters and establish that this vertical line intersects the elliptic curve at a third point O located at infinity, which represents the vanishing point.

In fact, it is possible to give a mathematical meaning to the point O by introducing a third variable z such that the equation for the elliptic curve becomes $y^2z = x^3 + axz^2 + bz^3$. Note that now all the terms in the equality are of degree three. This is extremely important, because it implies in a certain sense that it is impossible to distinguish the triple (x, y, z) from any of its non-zero multiples $(\lambda x, \lambda y, \lambda z)$, since
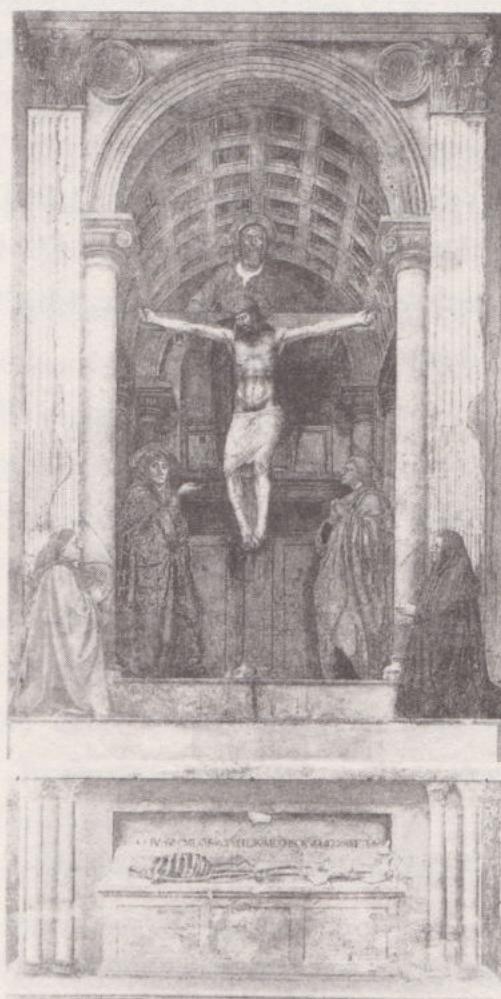
The Holy Trinity, a fresco by Masaccio (1401–1428), the first Renaissance painter to introduce mathematical perspective into his work to achieve the perception of depth.

if we substitute these values into the equation, the factor λ^3 can be simplified on both sides. This gives what are called *homogeneous* coordinates, which are represented as $(x: y: z)$ to indicate that two points that appear to be different at first glance, such as $(1: 2: 3)$ and $(2: 4: 6)$, are in fact the same – because one is a multiple of the other. Among other things, this allows us to assume that the coordinate z only takes the values 0 and 1. Returning to the equation, we can see that if we substitute z for 1, $y^2 = x^3 + ax + b$, so we recover the points of the elliptic curve that we were considering up to this point. However, if z is equal to 0, then $x^3 = 0$, hence x is also 0. As the three coordinates cannot simultaneously be cancelled, y must necessarily be non-zero. However, all the points $(0: y: 0)$ are the same since they are multiples of each other, hence we can assume that $y = 1$. Therefore, we obtain a new point $(0: 1: 0)$ that was not on the curve $y^2 = x^3 + ax + b$; this is our point O!

To recap: first we show that any non-vertical line that passes through two points on the elliptic curve also intersects it at a third. Now, thanks to the point at infinity, we know the same is true when the line is vertical. Therefore, we can define an operation between P and Q provided they are different points. However, what if they were the same? Is it possible to give a meaning to $P+P$? To see how to do this, imagine that we start with two different points, P and Q, and that we gradually bring Q closer to P. This means that the lines that join P and Q will also move. Somehow, the limit of these lines is the line tangent to the curve, which in the neighbourhood of P does not intersect it at any other point.
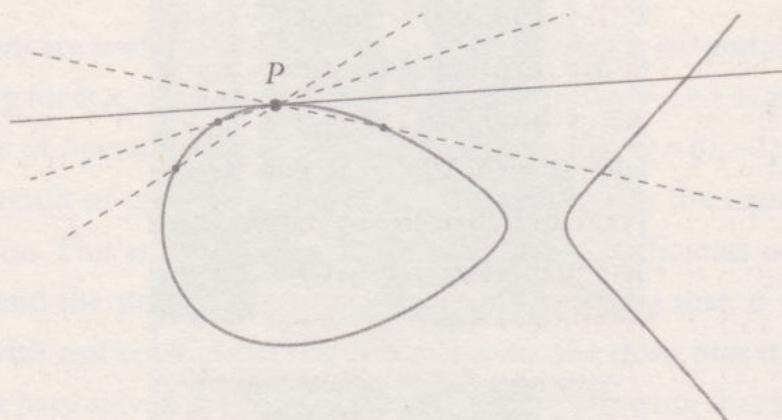
Straight line tangent to the curve at P.

Hence, instead of considering the line that joins P and Q, when the two points are equal, let us consider the line tangent to the curve at P. The same argument shows this line intersects the curve at another point PP. Using the symmetry with respect to the x axis, we obtain the sum $P+P=2P$.
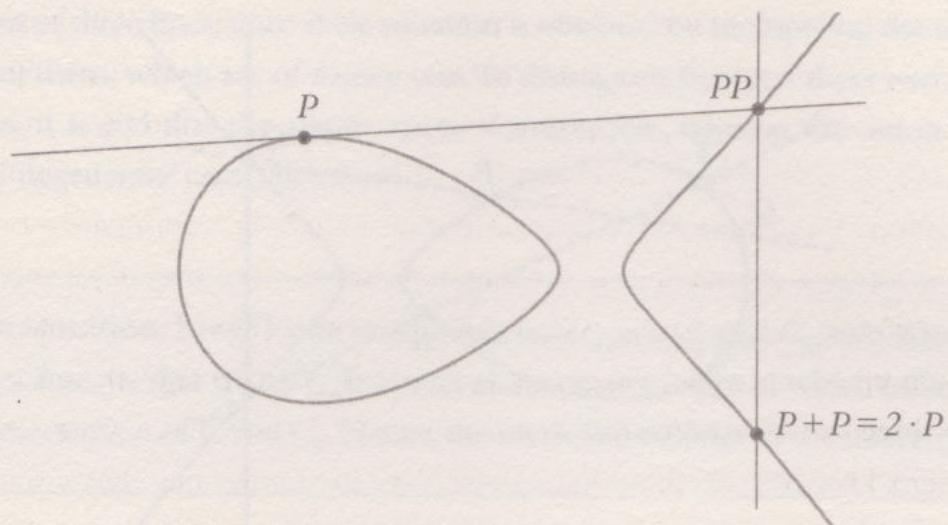
All that remains is a small subtlety. We have added the point O to our curve, now we must also define the result of adding O to another point on the curve. When we work using homogeneous coordinates, O has exactly the same status as the other points on the curve, hence it is possible to draw the line that passes through O and P and apply the previous procedure. However, in doing so, we always obtain $O+P=P$, hence O will be the identity element for the operation on the elliptic curve.

Therefore, we have defined an operation which, for each pair of points on the curve, regardless of whether they are different, associates a third. Let us show that it defines a group. Let O be the identity element. It is easy to calculate the inverse of a point P: it will be the symmetric point with respect to the x axis; let us represent it as P', since the line that passes through P and P' is vertical, and it intersects the curve at point O and we have $P+P'=O$. All that remains is to show that the operation is associative in order to conclude that the operation induces a group structure on the set of solutions to the equation $y^2=x^3+ax+b$.

Let P, Q and R be three points on the curve. We want to show that $(P+Q)+R=P+(Q+R)$. To do so, it is enough to show that the line l_1 joining $P+Q$ and R cuts the curve at the same point as the line l_2 that joins P and $Q+R$, since it is then only necessary to find the symmetric points. Let us first draw the line that joins P and Q and then look for the third point of intersection with the curve, which we have called PQ. Thanks to these two auxiliary lines, we obtain the point $P+Q$. We must now join $P+Q$ to R and see where this line l_1 cuts the curve. Let T be the point of intersection.
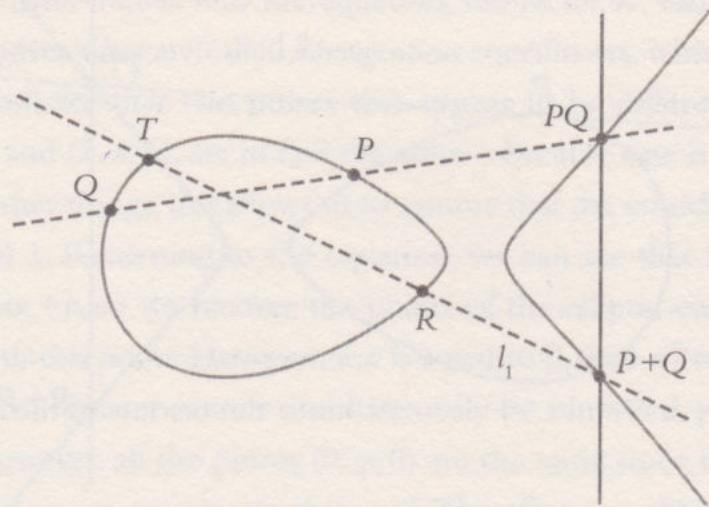
We will now calculate $P+(Q+R)$ on the same image. The line that joins Q and R cuts the curve at a third point, QR, the symmetry of which gives the value of $Q+R$. It is a case of showing that the line l_2 that joins $Q+R$ and P cuts the curve at point T:
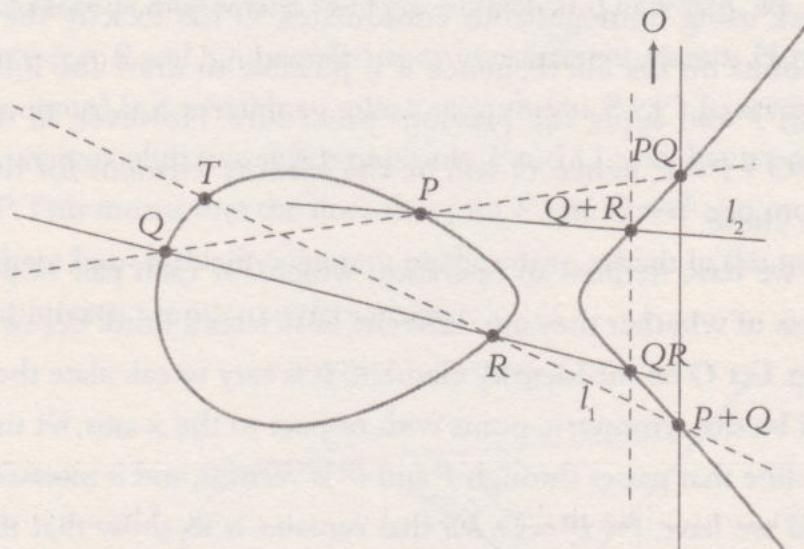
Let C_1 be the union of the three dotted lines. Bearing in mind that the 'vanishing point' O belongs to the line joining QR and $Q+R$, we can see that C_1 cuts the elliptic curve at the following points:

$$C_1 \cap C = \{O, P, Q, R, PQ, QR, P+Q, Q+R, T\},$$

of which the first eight also belong to the union of the solid lines, which we shall call C_2.

We can now use a classic result on the intersection of cubics on the plane. However, before doing so, let's recall that a cubic is a set of solutions to a third-degree equation in the variables x and y. For example, an elliptic curve $y^2 = x^3 + ax + b$ is cubic, but so is

the union of three lines, since their equation is obtained by multiplying the equations of each of them, which are of degree one. To distinguish between these two different situations, it is said that the elliptic curve is irreducible, whereas the union of three lines is a 'degenerate' case. Therefore:

Proposition: Let C be an irreducible cubic, and C_1 and C_2, two arbitrary cubics. Assume that C and C_1 intersect at nine points, eight of which belong to the intersection of C and C_2. Hence, the ninth also belongs to the intersection.

Applying the result to the elliptic curve, to C_1 and C_2, we can see that the point T belongs to C_2. Now though, the only point that still needed to be considered in the calculation of $C_2 \cap C$ was the point of intersection of the line joining P and $Q+R$ which can only be T, as we wished to show. Thus concludes the proof of associativity and also of the fact that the operation we have defined induces a group structure. We can also see that it is an abelian group, since the geometric construction of the sum $P+Q$ is based on the line joining P and Q, and this line is independent of the order in which we consider the points.

Hence, the rational points of the elliptic curve, which we shall denote as $E(\mathbb{Q})$, have a group structure. In 1922, the mathematician Louis Mordell proved the following result in response to a question by Poincaré:

Mordell's Theorem: The abelian group $E(\mathbb{Q})$ is generated by a finite number of elements.

This means that there is a finite quantity of rational solutions to the equation $y^2 = x^3 + ax + b$ based on which it is possible to recover all the others by successively applying the group operation. As we have seen, a finitely generated abelian group is always of the form

$$\mathbb{Z}^r \times \mathbb{Z}/n_1 \times ... \times \mathbb{Z}/n_k.$$

The number of copies of the group of integers involved is referred to as the *rank* of the elliptic curve and is extremely difficult to calculate. In fact, one of the most

significant open problems at present (a million dollars awaits the person able to solve it!), the *Birch-Swinnerton-Dyer conjecture*, consists of identifying the rank with other analytic invariants. However, elliptic curves are not only useful for winning a million dollars: they were an essential ingredient in the proof of Fermat's last theorem and, thanks to them, it has been possible to improve public key cryptography.

*****

WEIL: My thesis involved showing that Mordell's result was true for curves with equations that were of a higher degree. However, the English mathematician suspected that a much stronger property was true. Not only was the group of solutions finitely generated, but it was finite, that is no copy of the integers could appear in the breakdown. This was the conjecture that Hadamard wanted me to prove, and which was not solved until 1983.

LÉVI-STRAUSS: Thank you, Mr Weil. Your explanations have opened the door to a new world for me. However, let me ask you a favour. Let's not change the method again! If we are study companions, it is to be able to speak to each other.

Chapter 6

The Music of the Spheres

For algebra, the palace of exact crystals

[…]

For music, that mysterious form of time.

Jorge Luis Borges, *Another Poem of Gifts*

LÉVI-STRAUSS: In the first volume of my *Mythologiques* I wrote that music is the "supreme mystery of the human sciences". Do you think you can explain everything with group theory?

WEIL: Let me tell you a story, Mr Lévi-Strauss. Many years ago I attended a concert with my wife in which one of the theatre assistants suddenly died from a heart attack. The orchestra stopped playing until the doctors arrived, but the concert resumed shortly after. There continued to be a great commotion among the public in our box; people couldn't stop whispering. When I asked them to be quiet, they found my actions extremely cruel. "In God's name, have you not seen what just happened? That man has died!" A competition then ensued to see who could give the strongest recrimination to my attitude. My response was simply that, "There are much worse ways to die than listening to Mozart." That's how I would have liked to have gone. Can you imagine the pleasure of dying while listening to music that is very far above us in its incomprehensible serenity, but which, for a brief instance, stops to remember us and comes within our reach? Neither group theory nor any other scientific approximation to art will ever explain that, but it is possible to explain some of the formal properties that contribute to the beauty of music.

LÉVI-STRAUSS: Mathematics is the most abstract science, just like music is the most abstract of the arts.

WEIL: You know that the relationship between mathematics and music is almost as old as philosophy. If we believe the legend, Pythagoras was passing in front of a smithy when he was captivated by the harmony of the blows of the hammers on the hot metal. Measuring the size of the different implements, he realised that the blows of two hammers were only consonant when the relationship between their lengths

was expressed using small natural numbers. If, for example, one hammer was double the length of another (2:1), the sound was an octave higher, whereas, if the relationship between the two lengths was, for example, three halves (3:2), we would obtain an interval similar to what is now referred to as a *fifth*. In general, all the sounds that can be expressed as ($n + 1:n$) were pleasant to the ear. When he returned home, Pythagoras continued his experiments until he convinced himself that the beauty of music was all a matter of correctly balanced proportions.

LÉVI-STRAUSS: And beauty is truth. It is at this point that the philosopher launches into what some might call his *tour de force* based on the belief that "All is number." If the proof that music is numbers is considered together with the concept of a universe made up of spheres that dance to the melody of a divine music, the most obvious consequence is that the balance of the cosmos rests upon a few mathematical principles.

WEIL: This ordered paradise would be destroyed with the discovery of irrational numbers. It appears that Hippasus of Metapontum died at the hands of his Pythagorean colleagues after revealing that not all magnitudes could be written as the quotient of two natural numbers. I recall that my sister Simone, in response to a long letter I wrote to her from prison in Ruan in March 1940, and which must have caused her a severe headache, confessed to me that she had always found that story ridiculous[1]. In her opinion, events had occurred in exactly the opposite manner: upon discovering that square roots made it possible to measure lengths, Pythagoras would have shouted: "All is number!"

LÉVI-STRAUSS: This would explain why generations of men not only clung to the concept of the 'music of the spheres' despite the discovery of the irrational numbers, but that they transformed it into one of the motifs that would run through the whole of Western thought. Had its influence not been so great, Kepler would not have raised so many objections when it came to the law that states that the orbits of the planets around the Sun are not perfectly circular but elliptical. How could a God that *geometrises* choose the least harmonic of the two options for the motion of the heavenly bodies?

WEIL: The funniest thing is that not even Kepler himself, who in a certain sense 'silenced the heavens', accepted the ultimate consequences of his work. After publishing his research in *Astronomia nova* in 1609, the scientist continued to work on the theory of the music of the spheres, this time linked to the Platonic solids. He would publish it ten

---

1 The reader will find André's letter in the first volume of his *Complete Works* (pp. 224–255), and the response from his sister in Simone Weil, *Œuvres*, Paris: Gallimard, 1999, pp. 568–575.

years later in his *Harmonices mundi*, a book plagued with esoteric nonsense that would go on to inspire one of Paul Hindemith's operas three centuries later. Only the difficult conditions under which it was written can excuse Kepler – in a short space of time, his sister died, his only patron and protector in the royal court was excommunicated, and the whole of the town of Leonberg rose up against his mother, who was accused of witchcraft.

LÉVI-STRAUSS: Then we won't follow in his footsteps. Any serious conversation about harmony must begin with some sketches of physics. The fact that music reaches our ears through a series of waves that are transmitted through the air from a vibrating source cannot be overlooked. The frequency of a periodic process, as you know, is the number of times it is repeated per unit of time. It is measured in *hertz* (Hz), named after the German physicist Heinrich Rudolf Hertz (1857–1894). In the case of sound, the greater the frequency, the higher-pitched (or sharper) the sound that is heard. Based on these foundations, the convention is to use the letters C, D, E, F, G, A, B to refer to sounds with specific frequencies. For example, the musical note A corresponds to a wave with a frequency of 440 Hz.

WEIL: You know more about physics than I do! I would only like to add that the fact that it is a symbolic convention is reflected perfectly in the history of music. The A of Bach's organs vibrated at 480 Hz, whereas for Handel, around 1740, the figure was 422 Hz. There was a period during which performers competed among themselves to increase the frequency as much as possible so that the sound became increasingly sharp. Those to whom this genuine inflation was most damaging were the lute makers, who were inundated by the number of broken strings that had to be repaired every day, and of course the singers, who suffered problems with their voices. If I remember correctly, it was precisely the complaints from the latter that led the French government to fix a standard frequency by decree. The English did the same thing but with a different value, of course! It was not until 1939 that the 440 Hz standard to which we are accustomed was established at the Second International Conference for the Diapason. Who knows what the frequency of the music we listened to when we were young was, Mr Lévi-Strauss. Prior to this there had been attempts to standardise the note A at 439 Hz, but… 439 is a prime number and this complicates everything[2].

---

2 According to the explanation of a member of the *British Standards Institute*, "The BBC tuning note is derived from an oscillator controlled by a piezoelectric crystal that vibrates with a frequency of one million Hz. This is reduced to a frequency of 1,000 Hz by electronic dividers; it is then multiplied eleven times and divided by twenty-five, so producing the required frequency of 440 Hz. As 439 Hz is a prime number a frequency of 439 Hz [which does not appear in the breakdown of 1,000] could not be broadcast by such a means."

LÉVI-STRAUSS: Do you realise that, regardless of what we are talking about, we repeatedly return to the same idea? The frequency of a note in isolation doesn't matter; what matters is its relationship to the others. In fact, if all the frequencies of the notes of a score are multiplied by the same number, the ear would continue recognising the melody, lower or higher, depending on whether the factor chosen was less than or greater than one. This is why it is fundamental for us to understand the relationship between the frequencies of the notes of the scale. Let me remind you that, in addition to C, D, E, F, G, A, B, there are another five notes. Imagine we need to tune a piano. As you know, Mr Weil, it is made up of a series of white keys that correspond to the notes C, D, E, F, G, A and B, to which I have already referred. However, there are also smaller, black keys positioned between the white ones. These are the *accidental* keys. To describe them, we need to use the sharp symbol (#) or the flat symbol (♭). Adding a sharp to one of the seven 'white' notes has the effect of jumping to the key immediately to the right. Hence, the sharp notes allow us to go from the white keys to the black keys, except for two exceptions: E # and B #, which do not represent new notes. They are just other names for the notes F and C, since in both cases, the following key is white. Flats have the opposite effect. Adding a flat to a 'white' note jumps to the key to the left. For example, D♭ is the same as C #, and F♭ corresponds to E, since the closest key to the left of F is white. Depending on the situation, it will be easier to use sharps or flats.
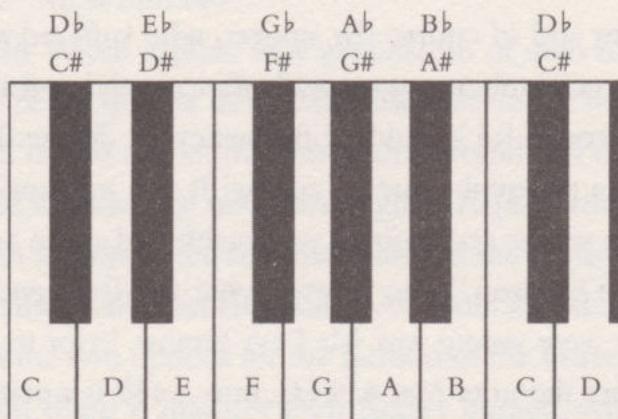
Piano keyboard.

Therefore, tuning a piano consists of identifying each of these notes with a certain frequency. As was the case for the note A, each era has proposed a different model. For example, the Pythagoreans constructed their scale by chaining together fifths. We say that a note is a fifth of another if, in order to reach it, it is necessary to pass over

eight keys of the piano. Hence, G is the fifth of C, since the keys C-C#-D-D#-E-F-F#-G stand between both notes. Similarly, the fifth of G is D. The name 'fifth' is justified by the fact that, starting from a white key, moving eight keys to the right almost always corresponds to moving five white keys, or in other words, counting five unaltered notes. However, note that if we start with B, we get F#, a black key – this is the exception. At any rate, repeating this process of chaining fifths together gives us the 12 notes of the scale.

WEIL: As I explained to you, Mr Lévi-Strauss, in the Pythagorean system, one note is the fifth of another if the ratio between their frequencies is three halves, or 1.5. Imagine, to simplify the calculations, that the note C corresponds to a frequency of 1 Hz. Since G is the fifth of C, its frequency will be 1.5 Hz. To calculate the frequency of D, we would need to multiply by 1.5 once again. However, this time we would get 2.25 Hz, which would mean that the note D is sharper than G. In fact, we have calculated the frequency correctly, but for a different octave. This is the frequency of the D that appears when we continue counting upwards G-A-B-C-D. It is necessary to lower the note by one octave, and we have already noted that this corresponds to dividing the frequency by two. Therefore, the frequency of D would be 1.125 Hz. We can use the same technique to calculate the frequencies of the notes:

$$C \rightarrow G \rightarrow D \rightarrow A \rightarrow E \rightarrow B \rightarrow F\#.$$

Now though, in the same way that we have 'moved up' by a fifth, we can 'move down' by dividing by 1.5 Hz. Since there are eight keys between F and C, F is the *descending* fifth of C. Dividing by 1.5 Hz and multiplying by 2 to recover the octave gives a frequency of 1.333… Hz. Continuing the descending process, we can calculate the remaining frequencies:

$$G\flat \leftarrow D\flat \leftarrow A\flat \leftarrow E\flat \leftarrow B\flat \leftarrow F \leftarrow C.$$

And if we wish to adapt them to the current ones, it is enough to find the factor that transforms A to 440 Hz and multiply all the other frequencies by this same number. However, there is a problem with the Pythagorean scale. Note that, applying our method, we have calculated the frequencies of the notes F# and G♭, but they are in fact the same! For the Pythagorean scale to allow for a perfect tuning of the piano, the two values must be the same. It is easy to see that this is not actually the case. Indeed, if we ignore the changes of octaves, the frequency of F# has been obtained

by multiplying by 1.5 six times, and the frequency of G♭ by repeatedly dividing by the same frequency. For the tuning to be perfect, the frequencies $(3/2)^6$ Hz and $(2/3)^6$ Hz could only be separated by a certain number of octaves. Put another way, the quotient of the numbers $(3/2)^6$ and $(2/3)^6$ would need to be a power of 2. But this is impossible, since the numbers 2 and 3 are relatively prime.

LÉVI-STRAUSS: That's why the *equal temperament* was introduced?

WEIL: Well, there were other methods before, such as the diatonic scale, but the equal temperament has been the most successful. A piano is tuned in this way when the ratio between the frequencies of the sounds of two consecutive keys, regardless of their colour, is always the same. For a mathematician, this means that if $f_1, f_2, f_3 \ldots$ represent consecutive frequencies starting from a given note, for example C, C#, D..., then the result of dividing f_2 by f_1 will be the same as dividing f_3 by f_2, which is the same as dividing f_4 by f_5, and so on. If I decide, for example to stop at f_{13}, we would have the inequalities:

$$\frac{f_2}{f_1} = \frac{f_3}{f_2} = \ldots = \frac{f_{13}}{f_{12}}.$$

LÉVI-STRAUSS: However, counting 13 keys starting from a given note gives the same note, just an octave higher.
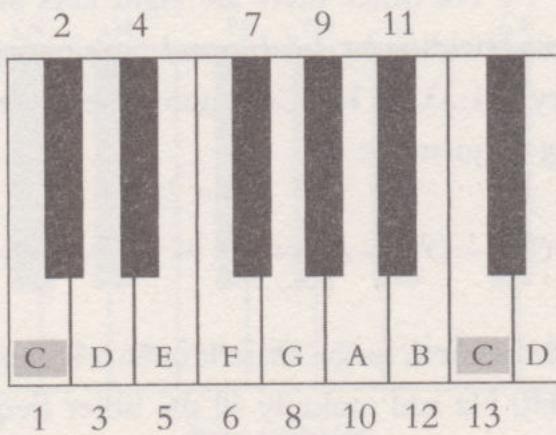
An octave on the piano.

WEIL: And going up an octave is the same as doubling the frequency, hence the quotient of f_{13} and f_1 is 2. Note that we can also write f_{13} divided by f_1 passing through

all the intermediate frequencies, such that those that appear as denominators are cancelled by those that appear as numerators:

$$\frac{f_{13}}{f_1} = \frac{f_{13}}{f_{12}} \cdot \frac{f_{12}}{f_{11}} \cdot \ldots \cdot \frac{f_3}{f_2} \cdot \frac{f_2}{f_1}.$$

Equal temperament implies that all the factors of the product are equal to the same quantity, let us call this d. Hence, f_{13} divided by f_1 gives 2, but also the result of multiplying the number d by itself 12 times. This gives the equation $d^{12} = 2$, according to which, given one frequency, the next is calculated by multiplying it by the twelfth root of 2, which is approximately 1.05946. For example, if the frequency of A is 440 Hz, as we have mentioned, the frequency of B (which is two keys above) will be 494 Hz, and the frequency of G (two keys below), will be around 392 Hz.

C	C#	D	D#	E	F
261.63	277.18	293.66	311.13	329.63	349.23

F#	G	G#	A	A#	B
369.99	392	415.30	440	466.16	493.88

Frequency table for the central notes of the piano.

LÉVI-STRAUSS: As a result, assigning A to the frequency 440 Hz is a convention, and once we have decided to do so, the other frequencies are determined.

WEIL: Always working with the hypothesis that an octave is divided into 12 notes, the frequencies of which have the same ratio – do not forget that. These are the foundations, but orchestras are not always tuned using the tempered note. Furthermore, all this has changed greatly in contemporary music; and this is to say nothing of other cultures governed by different systems. In Indian music, for example, there is no equal temperament…

LÉVI-STRAUSS: I'm embarrassed to admit that I have paid little interest to so-called ethnographic musics. It is certain that during my experiences in Brazil I had

the privilege of listening to wonderful melodies, which are now lost. I remember that the flutes of the Nambikwara Indians reminded me of the 'Ritual Action of the Ancestors' from Stravinsky's *Rite of Spring*. During the trip, I made a great deal of effort to transcribe the music I heard to the best of my abilities. Upon my return to France, a pianist helped me to improve the scores and interpreted them to allow me to choose between the ones that resonated most strongly in my mind. Do you know what happened next? The editor in charge of publishing them lost them in a taxi. Perhaps this disappointment lay behind the fact that I did not think seriously about music again until almost 30 years later, although there were few days in my life when I was not accompanied by a work by Ravel, Debussy or Chopin. One of his *Études* was of great use when it came to calming my anxiety in the jungle. Music is the thread that joins my *Mythologiques*. To begin with, I thought it was a good way of organising a complex discourse, with many variations on the same theme. We have all done it; you also used music in your memoirs, Mr Weil. The final chapter is a 'comedy opera', with a prelude, a fugue and an *intermezzo*. However, I soon understood that there was a more profound reason. At the point at which the novel replaced the civilising mission of ancient myths, without realising it, music came to occupy the role of an agonising mythology. This must be one of the keys to interpreting a work such as Wagner's *Tetralogy*.

WEIL: Getting back to the point, if you will allow me, let me remind you that a while ago, you yourself said that counting three keys from a given note, we returned to the same note one octave higher. An octave is divided into 12 units. Thanks to this principle, group theory can play an interesting role in the study of harmony. In fact, we use a single note, such as, A, to refer to different sounds related by octaves. Without going into greater detail, there are eight different As on the piano keyboard, and in principle we could continue to consider higher and lower octaves indefinitely, if it wasn't for the fact that the human ear can only distinguish a limited range of frequencies. According to the previous calculations, let A be any note with a frequency of 55, 110, 220, 440, 880, 1,760... This situation should not be completely new; cast your mind back, Mr Lévi-Strauss. When I mentioned *clock groups*, I explained to you that we identified six o'clock in the morning with six o'clock in the afternoon, six o'clock the following morning or six o'clock the previous afternoon. One octave higher, 12 hours later. One octave lower, 12 hours earlier. It's the same thing! For this reason, it is highly practical to roll the piano keyboard into what we shall call the *dodecaphonic circle*.
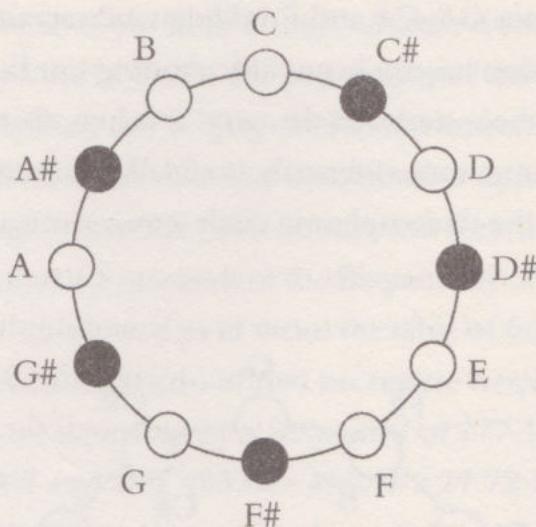
The dodecaphonic circle.

LÉVI-STRAUSS: The interval that separates each note from the following in the circle is called a *semitone*. As we would expect, two semitones make up a *tone*, and three semitones make up what is often known as a *minor third*. In fact, the classical tradition associates a name to each interval:

3	Minor third		8	Augmented fifth
4	Major third		9	Major sixth
5	Fourth		10	Augmented sixth
6	Tritone		11	Major seventh
7	Fifth		12	Octave

Note that a fifth is made up of seven semitones, which correspond precisely to the eight keys of the piano we counted starting from the note.

WEIL: Transposing a melody, as you know, consists of adding or subtracting a constant quantity of semitones for each note. Imagine that we need to raise the three notes that are repeated in the first bars of Beethoven's *Moonlight Sonata* by a fifth:

The first notes of Beethoven's Moonlight Sonata.

115

Because the notes are G#, C# and E, adding seven semitones to each gives D#, G# and B. The calculation has not been difficult using our fingers, but imagine if we had to transpose the whole sonata in this way! It is here that a musical model based on group theory becomes extraordinarily useful. What would you say if I told you that it suffices to turn the dodecaphonic circle seven semitones in an anticlockwise direction?
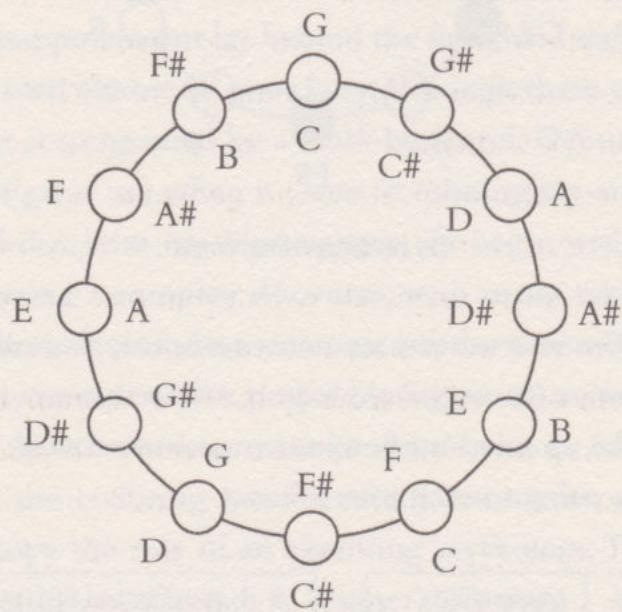
Transposition of the fifth.

Conserving the original notes in the inner part of the circle gives a correspondence that allows us to carry out the transposition without difficulty. Look how easy it is to do this with the beautiful *leitmotiv* of Fauré's *Pavane*.

With the new method, the sequence of notes

F#–G#–A–B–A–G#–A–F#–G#–A–G#–F#–G#–E–F#–F–C#

is transformed at the batting of an eyelid into

C#–D#–E–F#–E–D#–E–C#–D#–E–D#–C#–D#–B–C#–C–G#.

LÉVI-STRAUSS: Impressive, Mr Weil! However, there is something that intrigues me about all of this. First we said that the perception of the structure of a melody is not changed by multiplying all the frequencies by a common factor, and now we have begun to add semitones. Is it the case that the two operations are the same?

WEIL: An excellent question, Mr Lévi-Strauss. For sure, at the beginning of our conversation, we stated that the quotient of the frequencies of two consecutive notes was constant; this was what allowed us to write the table of frequencies starting with the note A. Note that the subtraction of two successive frequencies is not constant at all. While C and C# are separated by a frequency of $277.18 - 261.63 = 15.55$ Hz, the distance between A# and B is $493.88 - 466.16 = 27.72$ Hz, almost double! To transform the products into summations and quotients into subtractions we need to use *logarithms*. It appears that Isaac Newton was first to realise their usefulness in musical calculations. Allow me to quickly refresh your memory; perhaps the last time they were explained to you was almost a century ago. Given two positive numbers a and b, the logarithm of a with respect to base b is written as $\log_b(a)$ and is the quantity to which b must be raised to obtain a. In other words: c is the logarithm of a with respect to base b if the numbers a, b and c satisfy the relationship $b^c = a$. For example, we know that $\log_2(4) = 2$ and $\log_2(8) = 3$, since $2^2 = 4$ and $2^3 = 8$, although the calculation is not always so easy. All you need to know is that logarithms are an operation that transforms quotients into subtractions:

$$\log_b\left(\frac{x}{y}\right) = \log_b(x) - \log_b(y).$$

Continuing with our example, if the base was $b = 2$, and the numbers in the formula were $x = 8$ and $y = 4$, its quotient would be 2, such that the term on the left would represent $\log_2(2) = 1$. On the other hand, we have already calculated $\log_2(8) = 3$ and $\log_2(4) = 2$. Using the formulae, we can see that this is the case, since $1 = 3 - 2$. The general proof is deduced from the basic properties of powers, try it!

Now though, we must imagine that the quotients of two consecutive frequencies are the same. This will still be the case if we apply the logarithm as follows:

$$\log_b\left(\frac{f_2}{f_1}\right) = \log_b\left(\frac{f_3}{f_2}\right) = \ldots = \log_b\left(\frac{f_{13}}{f_{12}}\right).$$

Based on the formula above, we can deduce that

$$\log_b(f_2) - \log_b(f_1) = \log_b(f_3) - \log_b(f_2) = \ldots = \log_b(f_{13}) - \log_b(f_{12}),$$

and this holds for any positive value of b. Imagine I choose one in particular: the 12th root of 2, the number d that satisfies the equation $d^{12} = 2$. A while ago I explained to you that each of the quotients of the two successive frequencies was d, hence, taking logarithms in base d, gives:

$$\log_d\left(\frac{f_2}{f_1}\right) = \log_d\left(\frac{f_3}{f_2}\right) = \ldots = \log_d\left(\frac{f_{13}}{f_{12}}\right) = \log_d(d) = 1,$$

since the exponent to which d must be raised to give d is one. Hence, I can use the expression that transforms the logarithm of a quotient into a subtraction of logarithms to deduce that:

$$\log_d(f_2) - \log_d(f_1) = \log_d(f_3) - \log_d(f_2) = \ldots = \log_d(f_{13}) - \log_d(f_{12}) = 1.$$

LÉVI-STRAUSS: What does all this mean? You've lost me!

WEIL: Ah, you were the one who asked for an explanation… I will now summarise what I wanted to say with these calculations. If, instead of concentrating on the frequencies $f_1, f_2 \ldots$ in their own right, we change the scale and deal with the logarithms with respect to base d of the frequencies, $\log_d(f_1), \log_d(f_2)$, going from one note to the next consists of adding a unit. In other words, a semitone!

LÉVI-STRAUSS: Up to this point we have ignored an essential fact. Looking at the circle of transposition, one could imagine that all the notes are used equally, but it is clear that the subset formed by the seven white keys C, D, E, F, G, A, B plays a dominant role. After all, this sequence is constructed in an extremely strange way. To go from C to D and D to E it is necessary to add a tone, but to go from E to F we only need to add a semitone, and there is no signal on the piano or the stave that indicates this. We then continue adding tones to go from F to G, G to A and A to B, but the interval between B and C once again breaks the symmetry:

$$C \xrightarrow{1} D \xrightarrow{1} E \xrightarrow{1/2} F \xrightarrow{1} G \xrightarrow{1} A \xrightarrow{1} B \xrightarrow{1/2} C.$$

This is the 'C major' key. We can construct new, equivalent scales from any note reproducing the series of intervals 1, 1, 1/2, 1, 1, 1, 1/2. In general, it will be necessary

to place accidentals. Think of Shostakovich's *String Quartet No. 3*. As part of the title, we can see the words 'F major'. This means that the dominant note in the score is not C, but F, hence the scale is reconstructed beginning with F. We want the pattern 1, 1, 1/2, 1, 1, 1, 1/2 to be preserved. From F to G and G to A there is one tone, very good, but from A to B there is not a semitone, as we would like to have, but a whole tone. Hence, instead of B we must consider the note one semitone below, in other words B♭. Let's continue: from B♭ to C, C to D and D to E there is a tone, and to finish, the interval between E and F consists of a semitone, as we wanted. The scale for 'F major' is obtained by substituting B with B♭, which is often indicated beside the key on the stave, to avoid having to write the accidental every time the note B appears on the score:
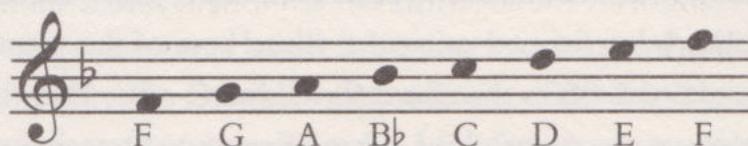
Scale in F major.

In this case, it has only been necessary to place one accidental, but consider how many we would need if we wished to begin the scale with F#, such as in Mahler's extraordinary *Symphony No. 10*, which he never had time to finish. From F# to G there is a semitone and we want there to be a tone, hence we must begin by changing G to G#. Now from G# to A there is just one semitone, so it is also necessary to go to A#. From A# to B there is a semitone, no problem here. However, the interval between B and C also consists of a semitone, when it should really be a whole tone: let us use C#. This means that the distance D is reduced to a semitone, meaning that it is also necessary to alter D, and the same thing happens with E. Finally, from E# to F# there is a semitone (we recall that E# was another name for F), as we wanted. Therefore, to construct the scale 'F-sharp major', we have had to change six out of seven notes.
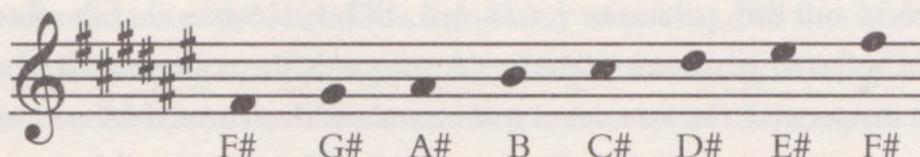
F-flat major scale.

WEIL: What your explanation makes clear, Mr Lévi-Strauss, is that the transpositions of a *fourth* (five semitones) are very sweet – almost imperceptible – because they only modify one note on the standard scale. When we want to make a smooth transition between two tonalities, it is useful to pass through various intermediate fourths. This is always possible since [5] generates the clock group in the sense that all its elements can be obtained by repeatedly adding [5]. For example, transposing a minor third (three semitones) is the same as transposing three fourths, since [5]+[5]+[5]=[3].

The opposite occurs with the *tritone* (six semitones). Since [6]+[6]=[0], applying the transposition twice returns us to the starting point. Surely you have heard the term *diabulus in musica*. During the Middle Ages, the church prohibited the use of the tritone on the grounds that it was an interval of such dissonance, that it turned the thoughts towards the impure – it could only be the work of the devil. One of the places in which the tritone appears naturally is in the chord B. Remember that the classic chords are formed using the white keys of the piano, ascending in pairs. For example, C d E f G is the chord for C, and G a B c D, is the chord for G. Note that in both cases, the first and last notes are separated by seven semitones. This property is shared by all chords, except those that start with B, since the total length of B c D e F is six semitones – the cursed tritone. Here is the 'devil in the music'! We needed to wait until the baroque period for the prohibition to be relaxed, and for the tritone to begin to appear in harmonies, initially only as a transitional chord, that would immediately be resolved into one of the other six.

LÉVI-STRAUSS: That would change with the arrival of the Romantics. One of the first pieces of music to exploit the potential of the tritone was Franz Liszt's *Dante Sonata*. Its first theme is composed in 'D minor'.

Thus far I have only referred to major keys; let me now briefly explain what the adjective 'minor' means. Consider the scale C D E F G A B once again. When we roll it up into a circle, a natural question is to ask what happens if we rotate the notes? We obtain, for example, the scale A B C D E F G, which no longer represents the sequence of intervals 1, 1, 1/2, 1, 1, 1, 1/2, meaning that it is no longer equivalent to the one we started with. Hence, it is worth investigating what happens when the semitones are placed in other positions. In the example, the semitones appear in the second and fifth positions: 1, 1/2, 1, 1, 1/2, 1, 1. Scales that conform to this pattern are referred to as *minor*. Hence, 'A minor' is the scale that corresponds to 'C major'. In general, the associated minor scale is determined by counting three descending semitones from the first note. Therefore, 'D minor' is the scale that corresponds to 'F major':

C major	A minor	F# major	D# minor
C# major	A# minor	G major	F minor
D major	B minor	G# major	F minor
F♭ major	C minor	A major	F# minor
F major	C# minor	B♭ major	G minor
F major	D minor	B major	G# minor

The correspondence between major and minor keys.

A crucial observation is that the associated minor scale has exactly the same accidentals as the major, hence these are not sufficient to determine if a work is written in a major or minor key. It is necessary to consider other, more subjective criteria, such as the note on which the cadences of the melody tend to end.

WEIL: Your discourse on tonalities, Mr Lévi-Strauss, once again leads us to suspect that not all the notes of the dodecaphonic circle are equally important in a melody. Arnold Schönberg could not accept this idea. Hence, while Einstein was putting the finishing touches to his first theory of relativity, he composed a *Kammersymphonie* that began the deconstruction of tonal principles. The most extreme stances would not come until the 1920s, when the father of the *12-tone technique* undertook a programme to argue for the absolute equality of the 12 notes in any composition, that would culminate in the work of the Second Viennese School.

LÉVI-STRAUSS: I remember my first contact with the new music. From an early age, my father took me to the Palais Garnier (Paris Opera House) and other concert halls on Sundays. You must remember that my great grandfather on my mother's side was the violinist Isaac Strauss, who worked with Offenbach and had known Rossini. Something of this has remained in the family, but my history of music ended with Wagner. I discovered Schönberg, Alban Berg and Anton Webern with the passion for sounds that were being heard for the first time, but I don't think I have ever been able to get used to them. Not to speak of the *serialism* of composers such as Luciano Berio, who did not only defend the democracy of pitches, but also of durations and timbres; in short any quantifiable parameter. I find it frustrating, I would like to escape from the bewilderment that they arouse in me, since some of the voices of *Symphony* scream texts from my book *The Raw and the Cooked*. However, I suppose it is not so easy to stop being a man from the 19th century…

WEIL: It doesn't surprise me that these sounds seemed completely new to you, since many of the major works of 12-tone music were composed using a Latin square. You now know that this is nothing more than an arrangement of a set of symbols in a table – in this case the 12 musical notes – such that each row and each column contain them all. The first step consists of choosing a sequence made up of 12 notes, which is used to construct the rest of the Latin square by following a series of established rules. Hence, there are as many 'composition guides' as there are ways of choosing an order of the elements C, C#, D, D#, E, F, F#, G, G#, A, A# and B. This gives a total of 479,001,600 sequences.

LÉVI-STRAUSS: Less than Queneau's one hundred thousand billion poems…

WEIL: But still a reasonable number to allow composers to continue to live with the illusion of creative freedom, don't you think? As I mentioned, the method is carried out by choosing an order for the 12 notes, such as:

E–G–F#–A–G#–C–F–D–D#–C#–B–A#,

written as follows in the treble clef:
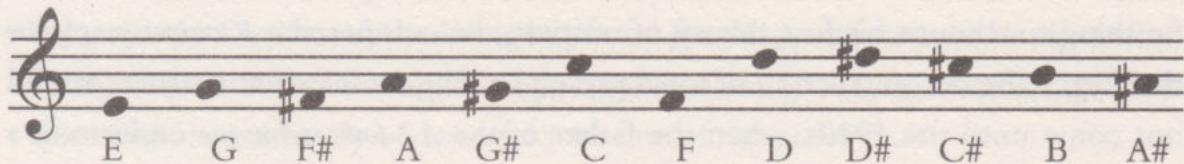
| E | G | F# | A | G# | C | F | D | D# | C# | B | A# |

and as follows in the bass clef:

| E | G | F# | A | G# | C | F | D | D# | C# | B | A# |

Hence, the first line of the table will be:

E	G	F#	A	G#	C	F	D	D#	C#	B	A#

Another way of writing it would be to identify each note with its position in the *clock group*. When it comes to carrying out the operations that make it possible to construct the whole Latin square based on the first line, it will be extremely useful to put 'noon' on the first note that we have chosen, or in other words to say

that E is the identity element for the group. Hence, we turn the clock until E is in the position normally occupied by C and copy out the numbers of the sequence:

```
                    [0]
         [11]        E         [1]
              D#          F
       [10]                      [2]
            D            F#
       [9]  C#                G  [
            C              G#
       [8]                       [4]
              B           A
                   A#
         [7]                 [5]
                    [6]
```
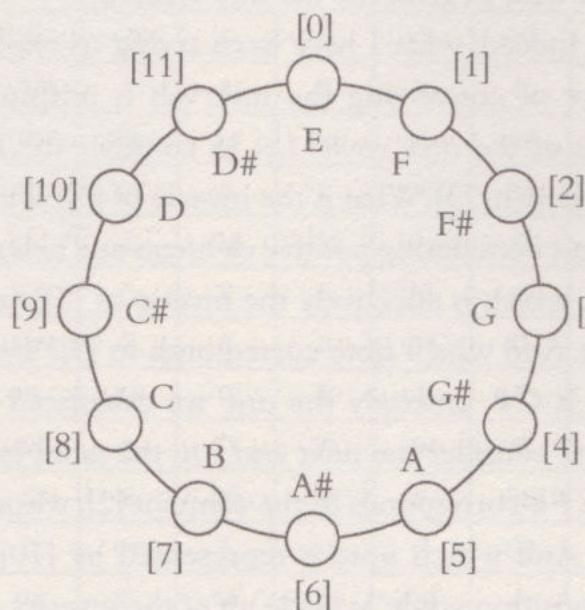
Remember that we write them between square brackets so that the notation makes it clear that a symbol such as [3] does not only represent the number 3, but also all the numbers obtained by adding and subtracting 12: 3, 15, 27, –9, –21… This allows us to translate the first line of the table into:

[0]	[3]	[2]	[5]	[4]	[8]	[1]	[10]	[11]	[9]	[7]	[6]

LÉVI-STRAUSS: Understood. What's the next step?

WEIL: Once we have the basic sequence, we complete the first column of the table by *inversion*. There will be a certain interval between each pair of notes in the first line. The method of inversion consists of reproducing this interval in the opposite direction, or in other words, downward if the first is ascending and upward if it is descending. For example, from E to G there are three ascending semitones (E-F-F#-G), therefore the inversion of the interval consists of counting three semitones downward: E-D#-D-C#. Hence, in the second space of the first column, we write C#. Another example: from G to F# there is an descending semitone, hence from C#, which we have just calculated, it will be necessary to ascend by a semitone, which gives us D. Continuing the process gives the first column:

E-C#-D-B-C-G#-D#-F#-F-G-A-A#.

Now though, Mr Lévi-Strauss, what does the word 'inverse' suggest to you?

LÉVI-STRAUSS: Given an arbitrary element of a group, its *inverse* is the element such that, composed with it, gives the identity element.

WEIL: Precisely! Indeed, what I have been trying to explain to you is that the harmonic procedure of converting the intervals is nothing more than finding the inverse elements of the *clock group*. Let us consider the first case. The note G corresponds to the element [3]. What is the inverse of [3]? We would be tempted to say [−3], but we are just considering positive elements and hence it is necessary to add 12. This gives us [9], which is effectively the inverse of [3], since [3]+[9]=[12]=[0], the identity element. And which note corresponds to [9]? Looking at the diagram, you will see that it is C#, precisely the one we calculated using the method of inversion! Let us now consider the next entry in the table, just in case you are not convinced. The note F# corresponds to the element [2], whose inverse is [10], since [2]+[10]=[12]=[0]. And which note is represented by [10]? D! Hence, the first column of the 'composition guide' is made up of the inverses of the elements of the fundamental sequence occupied by the first row:

$$[0] \; [9] \; [10] \; [7] \; [8] \; [4] \; [11] \; [2] \; [1] \; [3] \; [5] \; [6].$$

LÉVI-STRAUSS: Excellent, we now have a row and a column. I think I know how to form the rest of the table. Now we can calculate the interval that separates E from each of the notes in the column and transpose the first row to ensure the structure of the melody doesn't change. From E to C# there are nine semitones, and I will need to add this number to each of the notes in the initial sequence:

C#	E	D#	F#	F	A	D	B	C	A#	G#	G

WEIL: Precisely! And this transposition can be carried out by rotating the do-decaphonic circle nine semitones, as I explained a while ago, or by adding [9] to the elements of the first row. At any rate, the symbolic representation of the second row of the Latin square will be:

[9]	[0]	[11]	[2]	[1]	[5]	[10]	[7]	[8]	[6]	[4]	[3]

The same operation we have applied to the second row can be repeated with the remaining ten until the table is complete:

E	G	F#	A	G#	C	F	D	D#	C#	B	A#
C#	E	D#	F#	F	A	D	B	C	A#	G#	G
D	F	E	G	F#	A#	D#	C	C#	B	A	G#
B	D	C#	E	D#	G	C	A	A#	G#	F#	F
C	D#	D	F	E	G#	C#	A#	B	A	G	F#
G#	B	A#	C#	C	E	A	F#	G	F	D#	D
D#	F#	F	G#	G	B	E	C#	D	C	A#	A
F#	A	G#	B	A#	D	G	E	F	D#	C#	C
F	G#	G	A#	A	C#	F#	D#	E	D	C	B
G	A#	A	C	B	D#	G#	F	F#	E	D	C#
A	C	B	D	C#	F	A#	G	G#	F#	E	D#
A#	C#	C	D#	D	F#	B	G#	A	G	F	E

which, as we have seen, contains the same information as

[0]	[3]	[2]	[5]	[4]	[8]	[1]	[10]	[11]	[9]	[7]	[6]
[9]	[0]	[11]	[2]	[1]	[5]	[10]	[7]	[8]	[6]	[4]	[3]
[10]	[1]	[0]	[3]	[2]	[6]	[11]	[8]	[9]	[7]	[5]	[4]
[7]	[10]	[9]	[0]	[11]	[3]	[8]	[5]	[6]	[4]	[2]	[1]
[8]	[11]	[10]	[1]	[0]	[4]	[9]	[6]	[7]	[5]	[3]	[2]
[4]	[7]	[6]	[9]	[8]	[0]	[5]	[2]	[3]	[1]	[11]	[10]
[11]	[2]	[1]	[4]	[3]	[7]	[0]	[9]	[10]	[8]	[6]	[5]
[2]	[5]	[4]	[7]	[6]	[10]	[3]	[0]	[1]	[11]	[9]	[8]
[1]	[4]	[3]	[6]	[5]	[9]	[2]	[11]	[0]	[10]	[8]	[7]
[3]	[6]	[5]	[8]	[7]	[11]	[4]	[1]	[2]	[0]	[10]	[9]
[5]	[8]	[7]	[10]	[9]	[1]	[6]	[3]	[4]	[2]	[0]	[11]
[6]	[9]	[8]	[11]	[10]	[2]	[7]	[4]	[5]	[3]	[1]	[0]

LÉVI-STRAUSS: The twelve-tone table such as the one we have constructed could be used to compose the following fragment:

On the one hand, the lower stave reproduces the basic sequence of the first row in the key F, from which the rest have been obtained. On the other hand, the upper stave contains two melodies: the lowest reproduces the second column of the table, whereas the highest is the first row read from right to left. The possibilities are almost infinite!

WEIL: This is how the music of the spheres sounds today.

Appendix

Finite Abelian Groups with Two Generators[1]

This appendix provides a full proof of the theorem of the structure of finite abelian groups generated by two elements to which André Weil refers in his dialogue with Claude Lévi-Strauss (page 73).

> **Theorem:** A finite abelian group generated by two elements is isomorphic to a cyclic group or a direct product of two cyclic groups.

Before we go into details of the proof, let us recall the concept of isomorphism of groups, which we mentioned briefly on page 57.

Isomorphisms of groups

Let G and H be two groups whose operations we shall denote using the symbols $*$ and $\bullet$ respectively. Let e_G and e_H be their identity elements.

> **Definition:** A *homomorphism* between G and H is a function $\varphi: G \rightarrow H$, which, to each element g in G, associates an element $\varphi(g)$ in H (the *image* of g), such that the following conditions are satisfied:
>
> (i) The function φ transforms the identity element of G into the identity element of H, or rather: $\varphi(e_G) = e_H$.
> (ii) The result of multiplying two elements of G and then calculating the image of the product is the same as first applying φ to each of these, then applying the operation in H: $\varphi(a*b) = \varphi(a) \bullet \varphi(b)$.

An immediate consequence of this definition is that homomorphisms 'respect' the inverse elements, in other words: $\varphi(g^{-1}) = \varphi(g)^{-1}$, for any g in G. Effectively, $g * g^{-1} = e_G$, meaning that $\varphi(g * g^{-1}) = \varphi(e_G) = e_H$ thanks to condition (i). On the other hand, property (ii) guarantees that $\varphi(g * g^{-1}) = \varphi(g) \bullet \varphi(g^{-1})$. Putting both results together gives $\varphi(g) \bullet \varphi(g^{-1}) = e_H$, and the same holds if we switch the order of $\varphi(g)$ and $\varphi(g^{-1})$. Hence, $\varphi(g)$ is the inverse of $\varphi(g^{-1})$.

Homomorphisms are a fundamental tool when it comes to comparing two groups to see if they are different. A particularly important case is when both groups are indistinguishable in terms of their structure, as is the case, for example, with the symmetry group S_3 and the group of operations that leaves an equilateral triangle invariant (page 56). To formalise the fact that they have the same structure, we introduced the notion of isomorphism.

Definition: We say that a homomorphism $\varphi : G \rightarrow H$ is an *isomorphism* of groups when the following properties hold:

(1) *Injectivity*: If a and b are two different elements of G, then $\varphi(a)$ and $\varphi(b)$ are two different elements of H.

(2) *Surjectivity*: Each element of H is the image of an element of G. In other words, given any h in H, there is a g in G such that $\varphi(g) = h$.

Thanks to the properties of homomorphisms, we can see that injectivity equates to this other condition (easier to verify in practice):

(1') The only element of G that φ transforms into the identity element of H is the identity element of G, in other words, if $\varphi(g) = e_H$, then $g = e_G$.

Indeed, first let us assume that (1) is true and that $\varphi(g) = e_H$. Since φ is a homomorphism, we know that $\varphi(e_G) = e_H$, hence g must be the same as e_G; otherwise two different elements would have the same image. Conversely, let us see what happens when the property (1') holds. Let a and b be two elements of G such that $\varphi(a) = \varphi(b)$. We want to show that $a = b$. First we use the property of elimination (see page 58) to rewrite the equality in the form $\varphi(a) \bullet \varphi(b)^{-1} = e_H$. Since φ is a

homomorphism, $\varphi(b)^{-1}$ is the same as $\varphi(b^{-1})$ and $\varphi(a) \bullet \varphi(b^{-1}) = \varphi(a * b^{-1})$. Hence, $\varphi(a * b^{-1}) = e_H$ and from (1') we can deduce that $a * b^{-1} = e_G$. Multiplying both sides by b we can conclude that $a = \mathrm{b}$.

Another observation that will be useful to us throughout the proof is that, given a homomorphism between two finite groups *of the same order* (or in other words with the same number of elements), to check if it is an isomorphism, it suffices to check just one of the two properties (injectivity or surjectivity) since the other can be deduced automatically (prove it!).

Let us also mention the following result:

> **Proposition:** A homomorphism $\varphi : G \to H$ is an isomorphism if and only if there is another homomorphism $\psi : G \to H$ such that the result of first applying φ and then ψ is the identity in G (in other words, the map that leaves all the elements of G unchanged), and the same occurs with the composition of ψ and φ changing G for H.

In fact, given φ, the function ψ is defined as follows: to each h in H, it assigns the only g in G such that $\varphi(g) = h$. We will say that two groups G and H are *isomorphic* when there is an isomorphism between them, and write $G \simeq H$.

Having covered these preliminary considerations, we can now prove the theorem of the structure. Hence let G be a finite abelian group with two generators. Our goal is to construct an isomorphism between G and a cyclic group, or a direct product of two cyclic groups. In the first part of the proof we will see that it is always possible to choose the generators in such a way that the order of one divides the order of the other.

Choosing suitable generators

Let us begin with a lemma on cyclic groups whose order is the product of two relatively prime numbers. To make the notation easier, from now on we shall omit the subscript index for the group when we write the identity elements and, instead of separating the terms of the operation using the symbol $*$, we will concatenate them.

> **Lemma 1:** Imagine that the order of an element a can be written as $n = mr$, with m and r being two relatively prime integers. Hence $<a>$ is isomorphic to the direct product of the cyclic groups $<a^m>$ and $<a^r>$, whose orders are r and m respectively.

Since m and r are relatively prime, Bézout's identity (page 91) guarantees the existence of two integers u and v such that $um + vr = 1$. Let us define the map

$$\varphi : \langle a \rangle \rightarrow \langle a^m \rangle \times \langle a^r \rangle,$$

that sends an element a^i of $<a>$ to the pair $((a^m)^{ui}, (a^r)^{vi})$. Since a is of order n, we know that $a^i = a^{i+kn}$ for any integer k, and the first thing we must show is that the images of a^i and a^{i+kn} are the same through the function φ. To do so, note that

$$(a^m)^{u(i+kn)} = (a^m)^{ui}(a^m)^{ukn} = (a^m)^{ui}(a^n)^{ukm} = (a^m)^{ui}e^{ukm} = (a^m)^{ui},$$

since $a^n = e$. The same holds for the second coordinate, allowing us to conclude that $\varphi(a^i) = \varphi(a^{i+kn})$. Hence, the map is well defined. We shall now see that it is a homomorphism of groups. The condition $\varphi(e) = e$ does not cause a problem, since substituting $i = 0$ into the formula that defines φ, gives

$$\varphi(e) = \varphi(a^0) = ((a^m)^0, (a^r)^0) = (e, e) = e.$$

With respect to the second property:

$$\varphi(a^i a^j) = \varphi(a^{i+j}) = ((a^m)^{u(i+j)}, (a^r)^{v(i+j)}) = ((a^m)^{ui}(a^m)^{uj}, (a^r)^{vi}(a^r)^{vj}) =$$

$$= ((a^m)^{ui}, (a^r)^{vi})((a^m)^{uj}, (a^r)^{vj}) = \varphi(a^i)\varphi(a^j),$$

since, when taking the direct product of two groups, the operations are carried out coordinate by coordinate (page 70). This shows that φ is a homomorphism. We shall now show that it is in fact an isomorphism. To do so, note that $<a>$ and $<a^m>\times<a^r>$ are groups of the same order. Effectively, the elements a^m and a^r are of the order r and m respectively, since $(a^m)^r = (a^r)^m = a^{mr} = a^n$ and the element a has order n by the hypothesis. Hence, the order of $<a^m>\times<a^r>$ is the product of r and m, or in other words n, and is the same as the order of $<a>$. Hence, it suffices to show that φ is injective, or that if $\varphi(a^i) = e$, then $a^i = e$. Now though, if $\varphi(a^i)$ is the neutral element, $a^{mui} = a^{rvi} = e$, this implies that n divides mui and rvi, hence it will also divide the sum of both numbers. However, as a consequence of Bézout's identity, we know $mui + rvi = (mu + rv)i = i$. Hence, n divides i, the same as saying $a^i = e$, and the map φ is injective. This concludes the proof of the lemma.

Note that the previous result also holds in the opposite direction: if r and m are two relatively prime integers, the direct product of two cyclic groups of order r and m is isomorphic to a cyclic group of order rm, since the lemma provides an isomorphism between $Z/r \times Z/m$ and Z/rm. Let us now see how we can use it to choose the generators of G such that the order of one divides that of the other. Let us begin with two arbitrary generators a and b. Recall that, since G is a commutative group, all its elements can be written in the form $a^i b^j$, for i and j integers that satisfy the conditions $0 \leq i < \text{order}(a)$ and $0 \leq j < \text{order}(b)$ (page 72).

Another more sophisticated way of expressing the same condition is the following: the function $\langle a \rangle \times \langle b \rangle \to G$ that sends the pair (a^i, b^j) to the element $a^i b^j$ of G is surjective. Of course, all the difficulty lies in the fact that there is no reason why it should also be injective; the representation $a^i b^j$ need not necessarily be unique and, upon considering all the terms $a^i b^j$, we would be counting certain elements of G more than once. We shall deal with this problem later.

Let us now consider the orders of a and b. Thanks to the fundamental theorem of arithmetic (page 89), both can be written as a product of prime numbers. The idea is to separate the factors into two blocks depending on whether they both divide or not the orders of a and b. To make the argument easier to understand, we shall limit ourselves to the situation in which there is just one prime number p that divides the orders of a and b (the general case is the same, but there are subindexes everywhere that make it hard to read). Extracting the maximum powers of p, we can write $\text{order}(a) = p^e m$ and $\text{order}(b) = p^f n$, for e and f, two positive integers. Furthermore, let us assume that $e \leq f$. Note that m and n are relatively prime, since if

there was another prime factor that divided both it would also divide the orders of a and b, and would necessarily need to be p. The same holds for p^e and m, and p^f and n.

Applying the lemma to the cyclic groups generated by a and b, we obtain isomorphisms $\langle a \rangle \simeq \langle a^m \rangle \times \langle a^{p^e} \rangle$ and $\langle b \rangle \simeq \langle b^n \rangle \times \langle b^{p^f} \rangle$. Hence:

$$\langle a \rangle \times \langle b \rangle \simeq \langle a^m \rangle \times \langle a^{p^e} \rangle \times \langle b^n \rangle \times \langle b^{p^f} \rangle \qquad (\star)$$

Let us consider the last three factors, of orders m, p^f and n respectively. Since m and p^f are relatively prime, the lemma states that the direct product $\langle a^{p^e} \rangle \times \langle b^n \rangle$ is isomorphic to a cyclic group of order $p^f m$. However, n and $p^f m$ are also relatively prime, hence we can once more apply the lemma to see that the product of the three factors is isomorphic to a cyclic group $<x>$ of order $p^f mn$. Let $y = a^m$, which is an element of order p^e. The formula $(\star)$ implies that the direct products $<a> \times <b>$ and $<x> \times <y>$ are isomorphic, hence there is a surjective map for $<x> \times <y>$ in G. Or, put another way, x and y generate G. It is now easy to see that $\mathrm{order}(y) = p^e$ divides $\mathrm{order}(x) = p^f mn$, since we assumed $e \leq f$. Thus we have proved the following lemma[2]:

Lemma 2: Let G be a finite abelian group generated by two elements. It is possible to choose the generators such that the order of one divides the order of the other.

Let us continue with the proof.

The order of the group

By the previous lemma, we can choose generators x and y of G such that $\mathrm{order}(y) = l$ and $\mathrm{order}(x)$ are multiples of l, written lk. Hence, all the elements of G can be written as $x^i y^j$, for $0 \leq i < lk$ and $0 \leq j < l$. However, if two powers of the generators were

---

2 In fact, our argument shows the following, more precise result: let G be a finite abelian group generated by two elements a and b. We write $\mathrm{order}(a) = p_1^{e_1} \ldots p_r^{e_r} m$ and $\mathrm{order}(b) = p_1^{f_1} \ldots p_r^{f_r} n$, where p_i are prime numbers, e_i and f_i are non-negative integers, and m and n are relatively prime. Then G is isomorphic to a group generated by two elements x and y such that $\mathrm{order}(x) = p_1^{h_1} \ldots p_r^{h_r} mn$ and $\mathrm{order}(y) = p_1^{g_1} \ldots p_r^{g_r}$, where $h_i = \max(e_i, f_i)$ and $g_i = \min(e_i, f_i)$ for each $i = 1, \ldots, r$.

the same, this way of writing them would not be unique. For example, if y^3 was equal to x^2, then $x^2 y^4$ and $x^4 y$ would be two different ways of referring to the same element. Let us use t to refer to the smallest positive integer such that y^t coincides with x^s for some integer s. We know that $t \leq l$, since $y^l = e = x^{lk}$.

With this new notation, each element of G is uniquely written as $x^i y^j$, where $0 \leq i < lk$ and $0 \leq j < t$. Indeed, if $x^i y^j = x^{i'} y^{j'}$ for some $0 < j' \leq j < t$, we would have $x^{i'-i} = y^{j-j'}$, that is: $y^{j-j'}$ would be a power of x. Since $j'-j$ is strictly less than t, it can only be zero, hence $j = j'$ and $i' = i$, since $x^{i'-i} = e$ with $-lk < i'-i < lk$. This shows that the order of G is the product of the two upper bounds between which the exponents i and j move, in other words, lkt.

The integer v

Let r be the order of the element y^t. Hence, $e = (y^t)^r = y^{tr}$. Since y is an element of order l, we know that $l \leq tr$. We would like to show that $l = tr$, such that it is necessary to exclude the case in which $l < tr$. Our argument is as follows: if $l < tr$, there would be an integer $u < r$ such that l lies between tu and $t(u+1)$, hence $tu < l < t(u+1)$. Let us consider the quantity $t(u+1)-l$. On the one hand, it is a positive integer less than t, since $0 < t(u+1)-l < t(u+1)-tu = y$. On the other, we have the equalities $y^{t(u+1)-l} = y^{t(u+1)} = x^{s(u+1)}$, since the order of y is l, and $y^t = x^s$. However, we have then shown that there is a positive integer less than t such that y raised to this number is the same as a power of x, which is absurd if we bear in mind the definition of t as the smallest integer with this property. The possibility $l < tr$ is hence excluded and we have $l = tr$. Hence, $e = y^l = y^{tr} = x^{sr}$.

We will need this small result to continue:

Lemma 3: Let g be an element of order n in a group G. Then n divides any integer d such that $g^d = e$.

It suffices to prove it for the case in which d is positive. Since n is the smallest positive integer such that g raised to this power is the identity element, we know that $n \leq d$. Hence, we can divide d by n to obtain $d = pn + r$, where $0 \leq r < n$ is the remainder of the division. Hence $e = g^d = g^{pn+r} = (g^n)^p g^r = g^r$, since $g^n = e$. Hence, $g^r = e$, which implies that $r = 0$, since otherwise, the order of g would not be n but r. This

concludes the proof. Since $x^{sr}=e$, lemma 3 states that order $(x)=lk$ divides the integer sr, or in other words: there exists a v such that $sr=lkv$. Substituting the value of l that we have just calculated, we have $sr=trkv$. Since r is the order of the element y^t, it is a non-zero number and, dividing both sides, we can conclude that $s=tkv$.

End of the proof

In this last section, we shall show that G is isomorphic to the direct product of the cyclic groups generated by x and $x^{-vk}y$, where v is the integer we have just defined. We are dealing with elements of orders lk and t respectively. In the first case there is nothing to prove. In the second, we can note that

$$(x^{-vk}y)^t=x^{-vkt}y^t=x^{-vkt}x^s=x^{s-vkt}=e,$$

since $y^t=x^s$ and $s=vkt$. If there was another integer $t'<t$ with the property $(x^{-vk}y)^{t'}=e$, we would thus have $y^{t'}=x^{-vkt'}$. However, this contradicts the choice of t as the smallest integer such that y^t is a power of x. Hence, $x^{-vk}y$ has order t, and the order of the direct product $<x>\times<x^{-vk}y>$ is lkt.

Consider the function $\varphi:\langle x\rangle\times\langle x^{-vk}y\rangle\rightarrow G$ that sends the pair $(x^i,(x^{-vk}y)^j)$ to the element $x^{i-vk}y^j$. Using a calculation extremely similar to that used in the proof of lemma 1, we can show that φ is well-defined and is a homomorphism of groups (fill in the details!). Since G and $<x>\times<x^{-vk}y>$ are of the same order, to see that φ is an isomorphism, it is sufficient to prove that it is injective, or in other words that $x^{i-vk}y^j=e$ implies $x^i=e$, and $(x^{-vk}y)^j=e$. The latter is equivalent to $y^j=x^{vkj}$, so y^j is a power of x. Using an argument essentially similar to the one that allowed us to prove lemma 3, we can see that j must be a multiple of t, hence there is a j' such that $j=tj'$. Substituting:

$$e=x^{i-vk}y^j=x^{i-vktj'}y^{tj'}=x^{i-(vkt)j'}x^{sj'}=x^{i-sj'}x^{sj'}=x^i,$$

since $y^t=x^s$ and $s=vkt$. Hence, $x^i=e$ as we desired. We have seen that G is isomorphic to the direct product of two cyclic groups. When their orders are relatively prime, it will be isomorphic to a cyclic group. This concludes the proof.

Bibliography

ARBONES. J., MILRUD, P., *Rhythm, Resonance and Harmony. The mathematics of music.* Barcelona, RBA, 2012.

AUBIN, D., "The Withering Immortality of Nicolas Bourbaki: A Cultural Connector at the Confluence of Mathematics, Structuralism and the Oulipo in France," *Science in Context*, 10 (2), 1997, 297-342.

BOURBAKI, N., "Foundations of Mathematics for the Working Mathematician", Journal of Symbolic Logic 14, 1949, 1-8. N.

—: *Theory of Sets*, Berlin, Springer, 2004.

—: "The Architecture of Mathematics", The American Mathematical Montly, 57 (4), 1950, 221–223.

CALVINO, I., "Quickness", in *Six Memos for the Next Millennium*, Cambridge MA, Harvard University Press, 1998.

ERIBON, D., LÉVI-STRAUSS, C., *Conversations with Claude Levi-Strauss*, Chicago, Chicago University Press, 1991.

FRESÁN, J., "The Castle of Groups. Interview with Pierre Cartier", EMS Newsletter, December 2009, 30–33.

JAMES, J., *The Music of the Spheres: Music, Science and the Natural Order of the Universe*, New York, Grove Press, 1993.

LÉVI-STRAUSS, C., *A World on the Wane* (originally published in French as *Tristes tropiques*), New York, Criterion Books, 1961.

—: *The Elementary Stuctures of Kinship*, Boston, Beacon Press, 1969.

—: *Look, Listen, Read*, New York, Basic Books, 1997.

SENECHAL, M., "The Continuing Silence of Bourbaki – An Interview With Pierre Cartier", *The Mathematical Intelligencer* 20 (1), 1998, 22-28.

WEIL, A., *Foundations of Algebraic Geometry*, American Mathematical Society, 1962.

—: *Number Theory. An approach through history from Hammurapi to Legendre*, Boston, Birkhäuser, 1994.

—: *Œuvres scientifiques: collected papers*, Berlin, Springer, 2009, 3 vols.

WEIL, S., *Œuvres,* Paris, Gallimard, 1999.

—: *At Home with André and Simone Weil*, Chicago, Northwestern University Press, 2010.

WRIGHT, D., *Mathematics and Music*, Providence, American Mathematical Society, 2009.

Index

Amazing Algebra
Group theory and its applications

The French thinkers André Weil and Claude Lévi-Strauss — the former a mathematician, the latter an anthropologist — are among the greatest intellectuals of recent times. Group theory, one of the fields of expertise of Weil, is explained by means of a fictional dialogue between the two men, throwing light on the study of the structures built by societies, and their rituals, as researched by Lévi-Strauss. The book presents an illuminating study of the confluence of mathematics and human behaviour, as well as vivid portraits of two geniuses.